

# SHMOO

Ganography 2018



# 17 teams this year!

*As of Noon*

Team
Three Blind Mice
FDG
3d printed badge clone
LMB
Poultrygeist
MONKEY TACOS!
Team Bivalve
Raccoon Dealers
Cyber Wombats

## Stage Prizes:

- 1: Three Blind Mice
- 2: Three Blind Mice
- 3: Team FDG
- 4:
- 5:

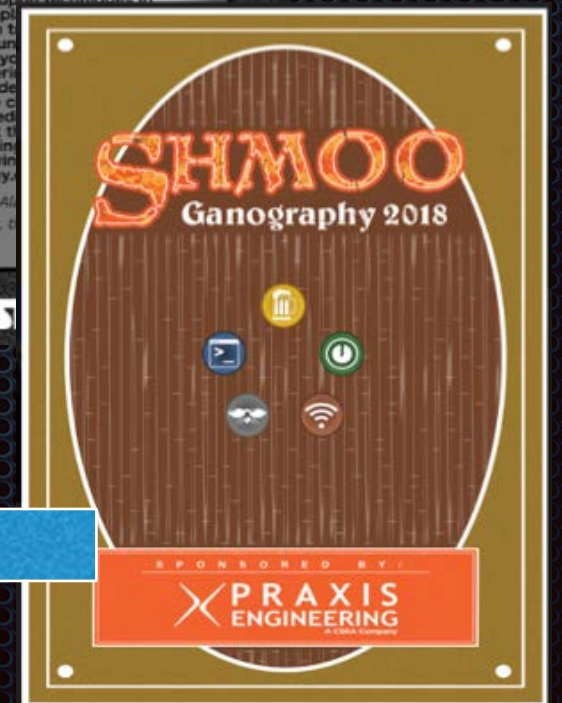
Team Tryhard
Team Big Gun
PwnEIP
Wahoo
will_hack_4_b00z
The Mana Dorks.
PettYeti's
anony-mouse



# Stage One: CYPHER

## Two-sided posters with stretched letters

- 4 posters designed as Shmooscon-inspired Magic cards
- Don't yell "Bow to my firewall!" at them!
- Backs have a hidden message, just tilt down or resize



GXXTHEXXMAGICTHEGATHERINGXXSTAGEXX



# Stage Two: EXPLOIT

## User Agent-Specific Website Rendering

- Visit contest website, /CARD
- Use Links and Vivaldi
  - Look at page source, search for “clue”
  - Vivaldi presents code, Links has clue



“A Browser  
for our  
Friends”

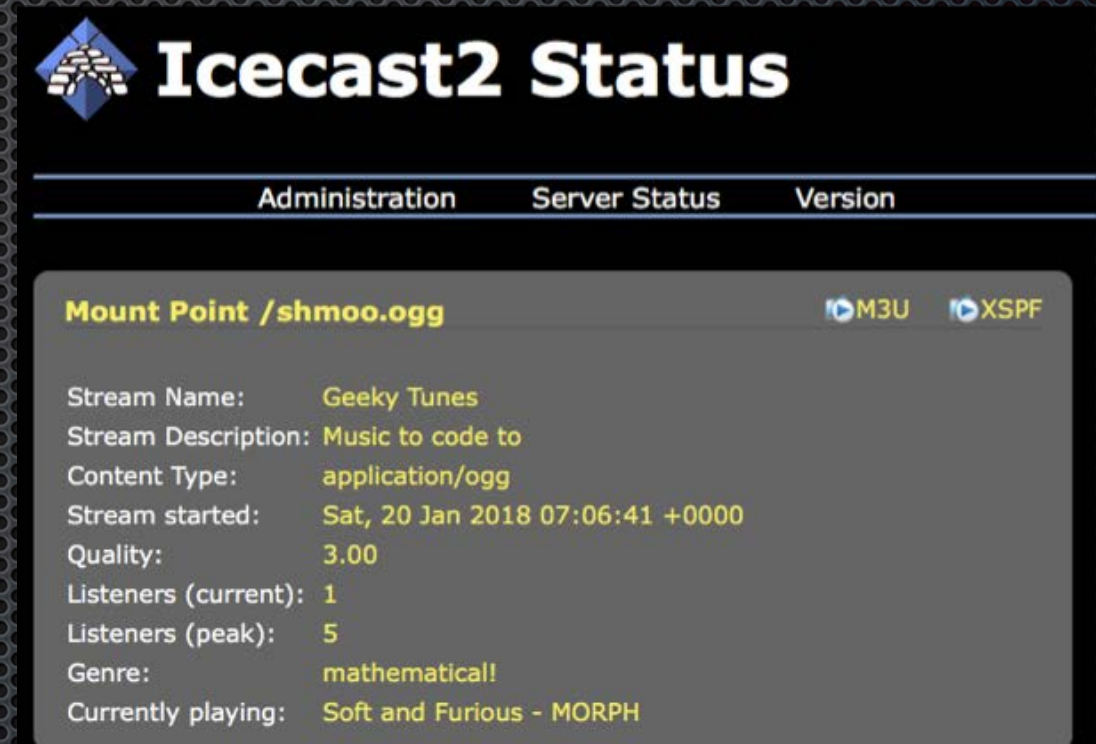
```
mjbowen — ubuntu@ip-172-26-2-109: ~ — ssh -i Downloads/LightsailDefaultPrivateKey-us-east-2.pem ubuntu@18.218.33.1...
~ — ubuntu@ip-172-26-2-109: ~ — ssh -i Downloads/LightsailDefaultPrivateKey-us-east-2.pem ubuntu@18.218.33.178
(p13 of 16)
><table><br><br><shmoogangoraphy clue="Magical tunes on shmoo.us.to:8000"></td></tr></table>
OK
```





# Stage Three: MORPH

## Data exfil via sweet Icecast techno streams

- A twist on previous our 2012 technique, this time streaming from AWS host
- Upper frequencies hold clue
- Song name is the code (from *Soft and Furious*)



The screenshot shows the Icecast2 Status page for the stream 'Mount Point /shmoo.ogg'. It includes a navigation bar with 'Administration', 'Server Status', and 'Version'. The main content area displays stream details: Stream Name (Geeky Tunes), Stream Description (Music to code to), Content Type (application/ogg), Stream started (Sat, 20 Jan 2018 07:06:41 +0000), Quality (3.00), Listeners (current: 1, peak: 5), Genre (mathematical!), and Currently playing (Soft and Furious - MORPH). There are also icons for M3U and XSPF feeds.

Icecast2 Status		
Administration	Server Status	Version
<b>Mount Point /shmoo.ogg</b>  		
Stream Name:	Geeky Tunes	
Stream Description:	Music to code to	
Content Type:	application/ogg	
Stream started:	Sat, 20 Jan 2018 07:06:41 +0000	
Quality:	3.00	
Listeners (current):	1	
Listeners (peak):	5	
Genre:	mathematical!	
Currently playing:	Soft and Furious - MORPH	

There's a fifth card, held in the digital plane...

There's a fifth card, held in the digital plane...



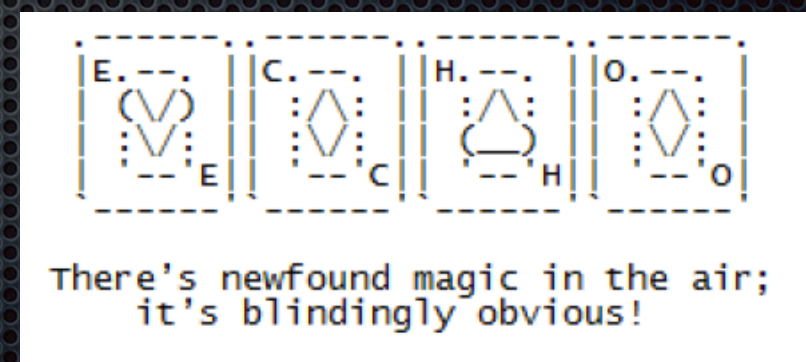
# Stage Four: ECHO

## PingFS network-hosted JPG file

- Using Erik Ekman's "true cloud storage" called PingFS
- Inspired by Steve Gibson's report on Security Now podcast
- "Storing" a JPG with a message hidden using *steghide*



No.	Time	Source	Destination	Protocol	Length	Info
186	2010-01-20 11:10:04.000000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 181)
187	2010-01-20 11:10:04.010000	172.16.42.7	172.16.42.1	ICMP	80	8000 Echo (ping) request id=0x0000, seq=1/256, ttl=64 (reply in 1)
188	2010-01-20 11:10:04.020000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=2/512, ttl=64 (reply in 1)
189	2010-01-20 11:10:04.030000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=3/768, ttl=64 (reply in 1)
190	2010-01-20 11:10:04.040000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=4/1024, ttl=64 (reply in 1)
191	2010-01-20 11:10:04.050000	172.16.42.7	172.16.42.1	ICMP	80	8000 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 230)
192	2010-01-20 11:10:04.060000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=1/256, ttl=64 (reply in 2)
193	2010-01-20 11:10:04.070000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=2/512, ttl=64 (reply in 2)
194	2010-01-20 11:10:04.080000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=3/768, ttl=64 (reply in 2)
195	2010-01-20 11:10:04.090000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=4/1024, ttl=64 (reply in 2)
196	2010-01-20 11:10:04.100000	172.16.42.7	172.16.42.1	ICMP	80	8000 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 230)
197	2010-01-20 11:10:04.110000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=1/256, ttl=64 (reply in 2)
198	2010-01-20 11:10:04.120000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=2/512, ttl=64 (reply in 2)
199	2010-01-20 11:10:04.130000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=3/768, ttl=64 (reply in 2)
200	2010-01-20 11:10:04.140000	172.16.42.1	172.16.42.7	ICMP	80	8000 Echo (ping) request id=0x0000, seq=4/1024, ttl=64 (reply in 2)



Was hosted on *shmoocon* wifi, shifted to PCAP :(



# Stage Five: HEXPROOF

## Data exfil via minor ZWave color changes

- Replaced hotel lamp bulb with RGBW LED blub
- Hosted *python-openzwave* on Odroid that periodically sent ZWave Color commands
  - ASCII string encoded in one color channel, byte per message
- RITSEC Blogpost steps you through all of it using cheap SDR to extract packets into Wireshark





Code words are all  
Magic keyword abilities

CYPHER

EXPLOIT

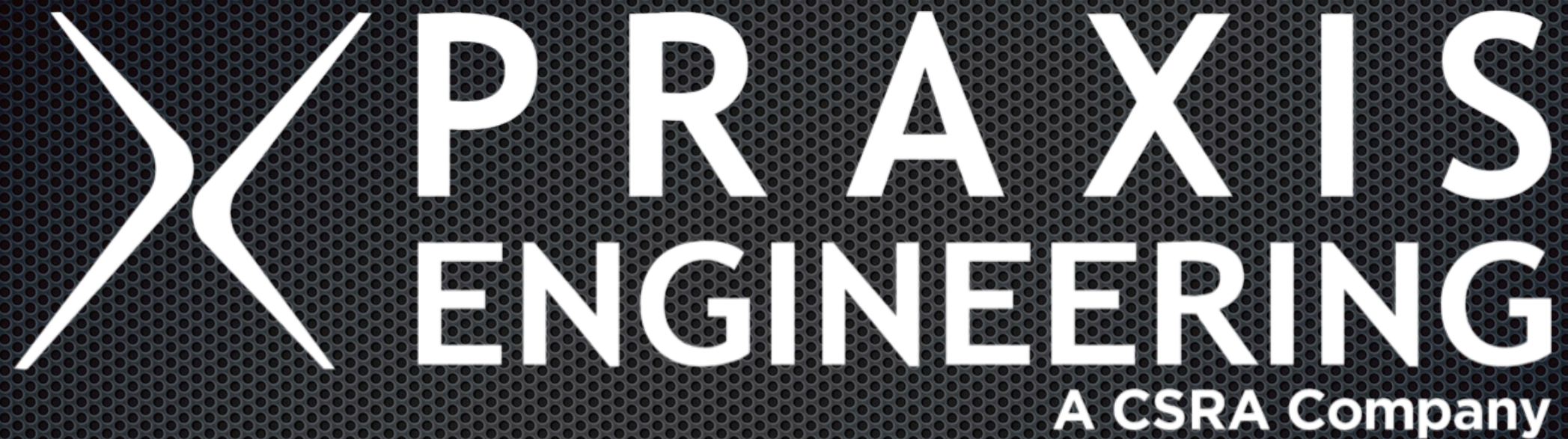
MORPH

ECHO

HEXPROOF



# Very Special Thanks



for their generous sponsorship,  
covering our expenses, materials,  
shirts and prize!



# Special Thanks

- Magic The Gathering, and their awesome planeswalkers
- NicBow Design Works, for our cool contest graphics
- No Starch Press, for coordinating gift certificates
- Not Just Signs, for super last-minute sign-printing
- FOSS Projects, like OpenZWave, PingFS, Coagula Lite, and Git Projects (LiptonB's wireshark, rtl-zwave)
- TOOOOL, for the confusion in using part of their logo
- Our Wives, for tolerating our annual hiatus
- Bruce & Heidi, for tolerating our endless shenanigan



[shmooganography@gmail.com](mailto:shmooganography@gmail.com)

Presentation will be available on the  
contest website soon.