fishnet SECURITY

Securely Enabling Business

SYNful Deceit: Stateful Subterfuge

Chris Patten
FishNet Security

Tom Steele
FishNet Security

Security Technology

Infrastructure

Security Integration

24x7 Support

MSS

Training

Information Assurance

Staff Augmentation

#/WHOAMI:CP

- Name: Chris Patten
- Job: Security Consultant
- Interests: Tech/Breaking $%&!
- Twitter: @packetassailant
- Email: cpatten@packetresearch.com
- Presentations/Articles:
    - OWASP, Black Hat, 6Labs, WSJ

fishnet SECURITY
Securely Enabling Business

#/WHOAMI:TS

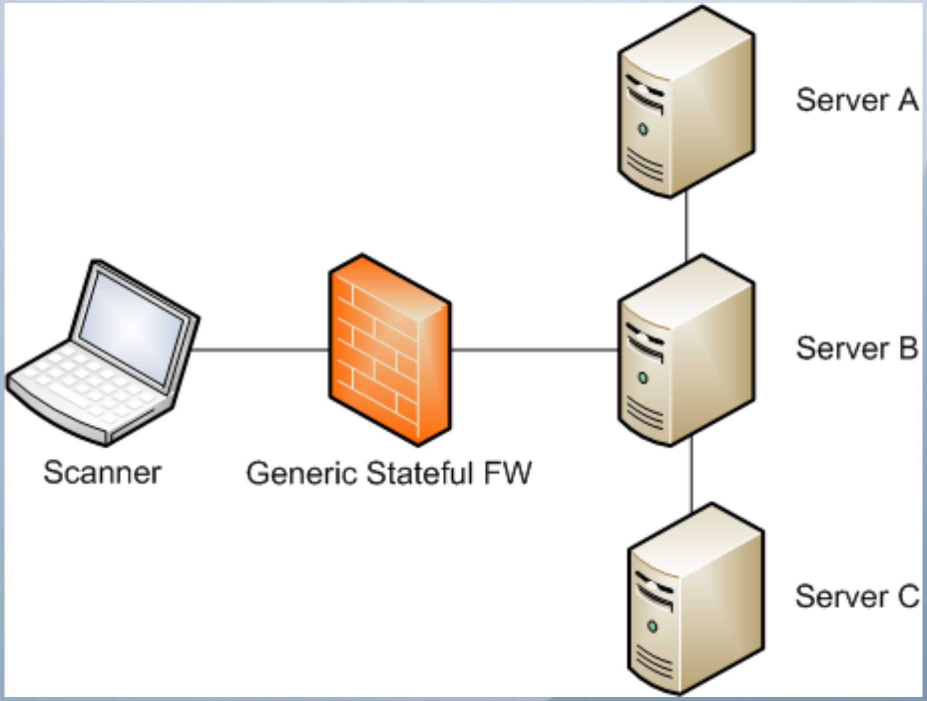
- Name: Tom Steele
- Job: Security Consultant
- Interests: Breaking Everything
- Twitter: @theL1on
- Email: tom@huptwo34.com
- Presentations/Articles:
    - Black Hat, 6 Labs

Service Discovery…It Works…

- When service scans are necessary
  - Vulnerability Assessments
  - Penetration Tests
  - Network Troubleshooting
- Numerous Tools Available
  - Fyodor’s Nmap
  - Kaminsky’s Scanrand
  - Jack C. Louis’ Unicornscan

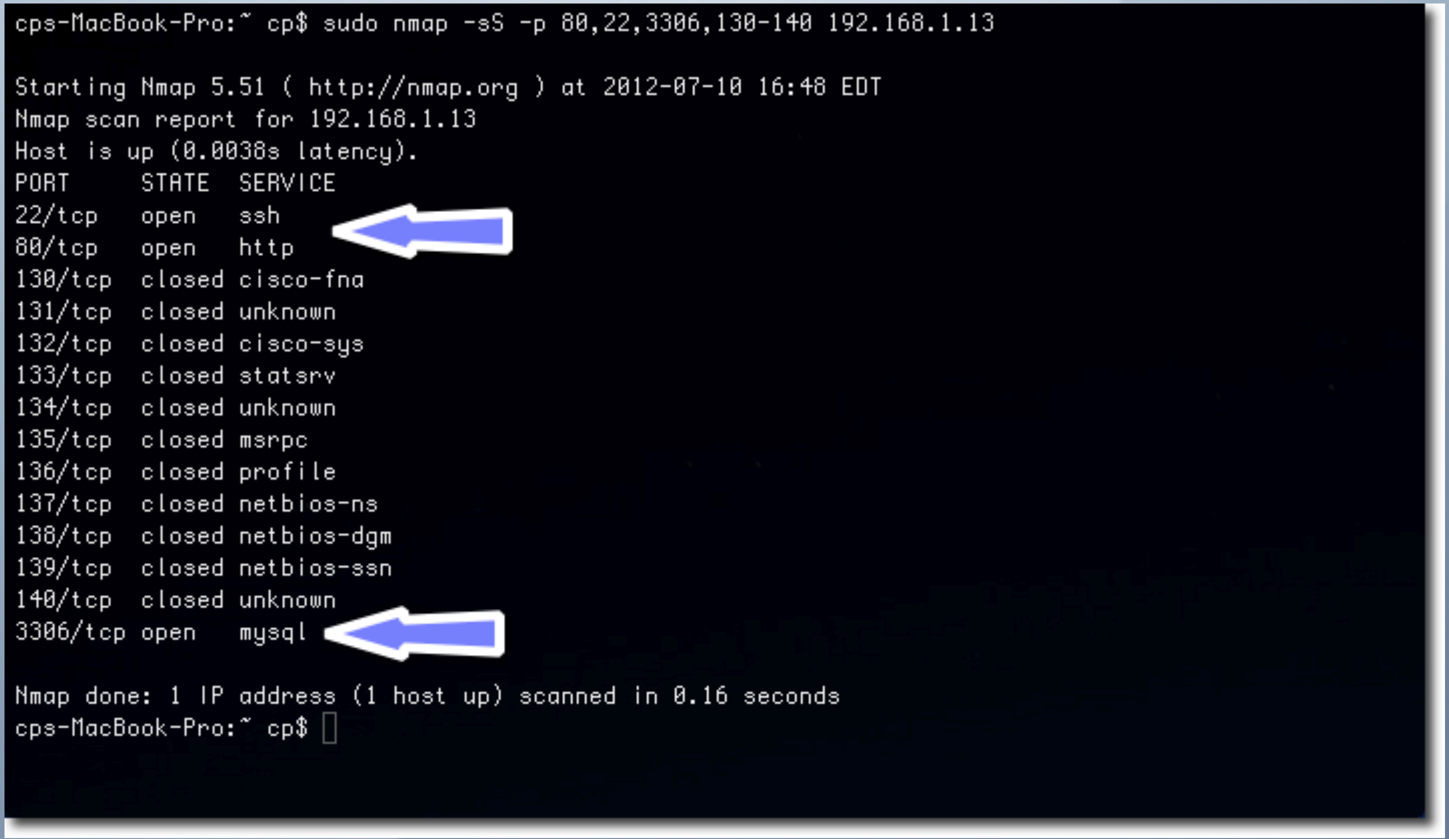
Securely Enabling Business

With a stateful firewall architecture…



Most of the time…

SYN Scans typically return open ports



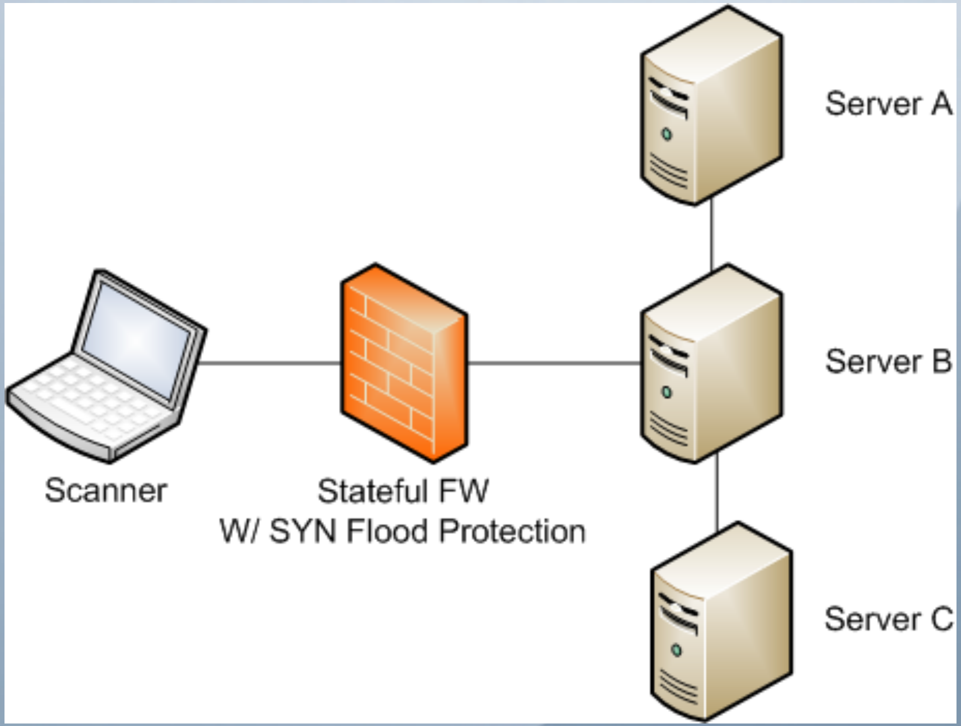
```
cps-MacBook-Pro:~ cp$ sudo nmap -sS -p 80,22,3306,130-140 192.168.1.13

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-10 16:48 EDT
Nmap scan report for 192.168.1.13
Host is up (0.0038s latency).
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
130/tcp  closed cisco-fna
131/tcp  closed unknown
132/tcp  closed cisco-sys
133/tcp  closed statsrv
134/tcp  closed unknown
135/tcp  closed msrpc
136/tcp  closed profile
137/tcp  closed netbios-ns
138/tcp  closed netbios-dgm
139/tcp  closed netbios-ssn
140/tcp  closed unknown
3306/tcp open   mysql

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
cps-MacBook-Pro:~ cp$
```

Sometimes…

- What about SYN Flood Protection
  - BSD PF Synproxy State
  - Netfilter/IPTables DELUDE Target
  - F5 SYN Check
  - Juniper’s SYN-Protector
  - Cisco’s TCP Intercept
- Difficult to identify relevant services
  - Creates two sessions
  - Acts as a broker to bridge sessions
  - Incomplete SYN scan transaction

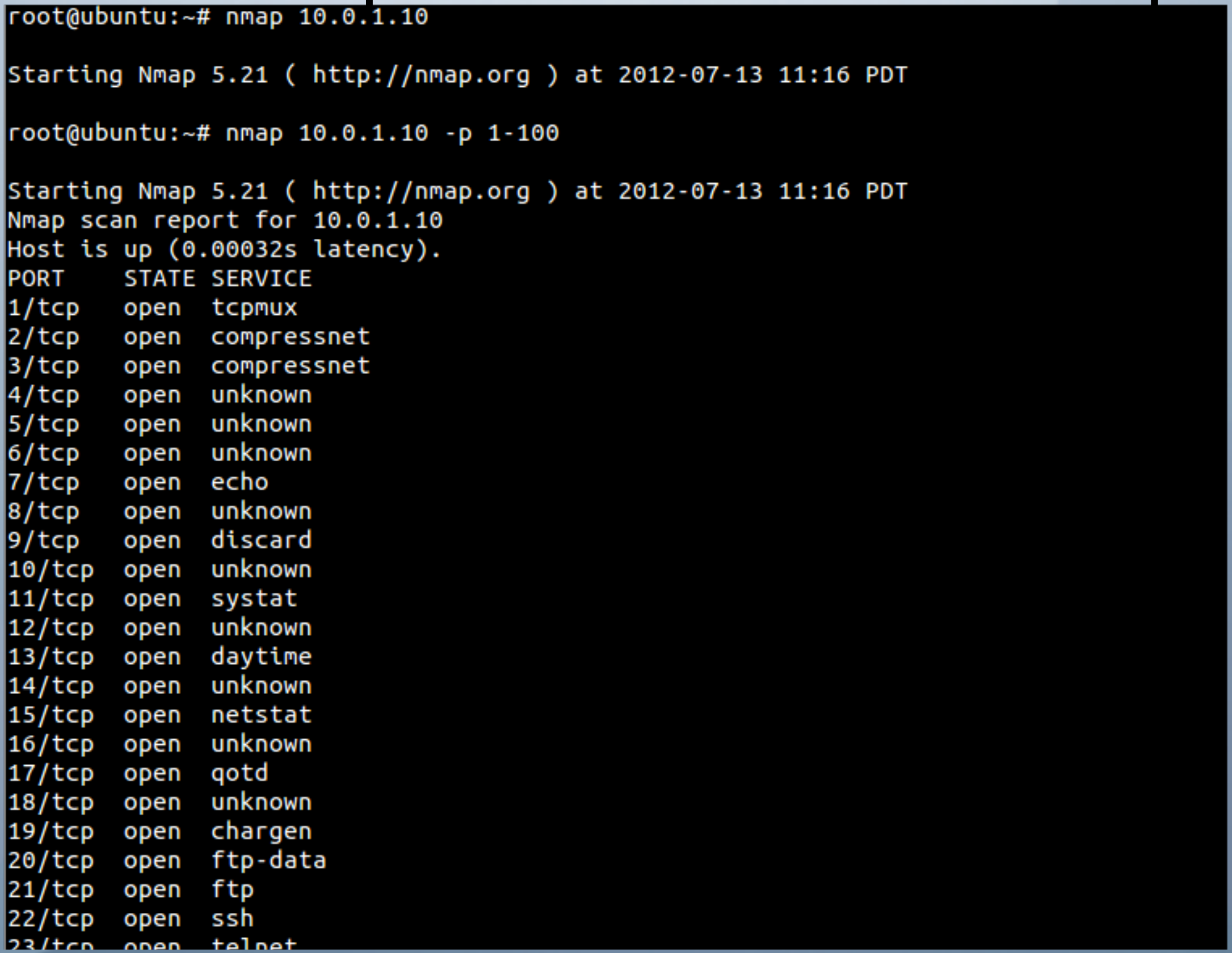
fishnet SECURITY
Securely Enabling Business

Again, but with SYN Flood enabled…



And then again, sometimes not…

SYN Flood protection returns all open



```
root@ubuntu:~# nmap 10.0.1.10

Starting Nmap 5.21 ( http://nmap.org ) at 2012-07-13 11:16 PDT

root@ubuntu:~# nmap 10.0.1.10 -p 1-100

Starting Nmap 5.21 ( http://nmap.org ) at 2012-07-13 11:16 PDT
Nmap scan report for 10.0.1.10
Host is up (0.00032s latency).
PORT     STATE SERVICE
1/tcp    open  tcpmux
2/tcp    open  compressnet
3/tcp    open  compressnet
4/tcp    open  unknown
5/tcp    open  unknown
6/tcp    open  unknown
7/tcp    open  echo
8/tcp    open  unknown
9/tcp    open  discard
10/tcp   open  unknown
11/tcp   open  systat
12/tcp   open  unknown
13/tcp   open  daytime
14/tcp   open  unknown
15/tcp   open  netstat
16/tcp   open  unknown
17/tcp   open  qotd
18/tcp   open  unknown
19/tcp   open  chargen
20/tcp   open  ftp-data
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
```

fishnet SECURITY
Securely Enabling Business

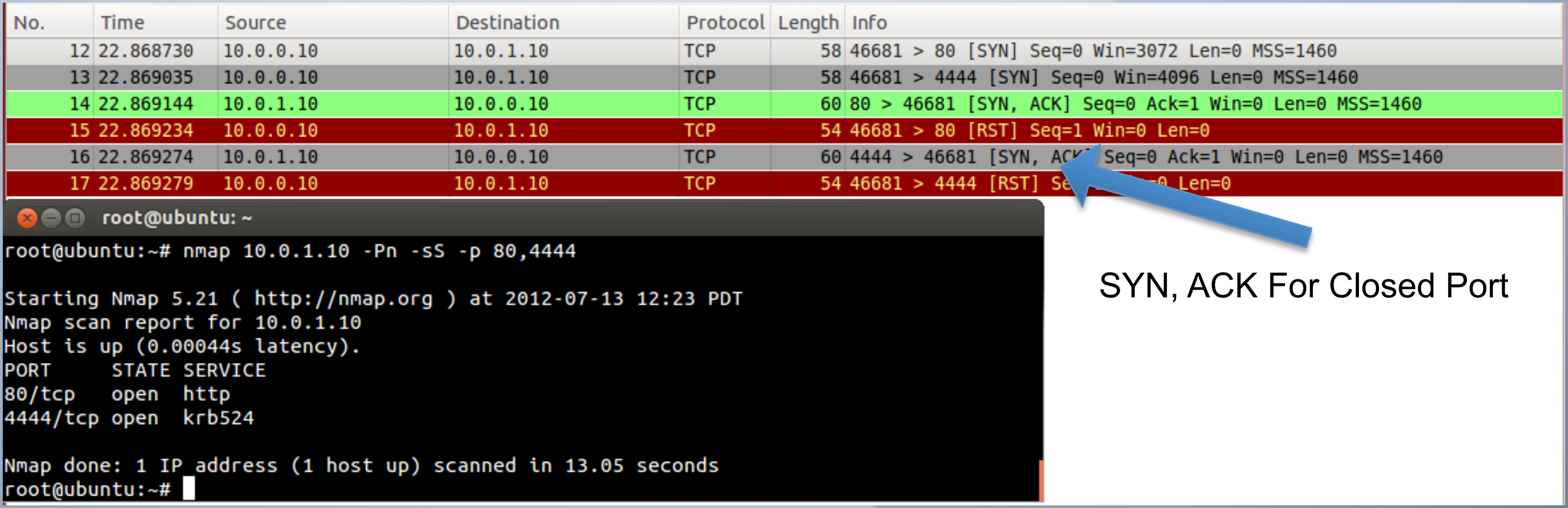
Misconceptions of the truth?...

- People say crazy @#%$!
  - Increase the packet delay
  - Perform a Connect Scan
  - Use a different scan (ACK, FIN)
  - Use version detection and grep
- Why this is often just crazy @#%$!
  - FW not allowing connections without state through
  - Connect Scan checks for 3-way handshake completion… not useful!
  - Version detection when every port is flagged as open is… slow!

What is SYN Flood Protection?…

- A proxy completing 3-way handshake
- A method to broker SYN connections
- Prevention of resource exhaustion
- Prevention from Spoofed Source IPs
    - SYN Cookies
    - Adjustable Queue Size
- But we just need a legitimate response

Setting it straight with a packet capture…



No.	Time	Source	Destination	Protocol	Length	Info
12	22.868730	10.0.0.10	10.0.1.10	TCP	58	46681 > 80 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
13	22.869035	10.0.0.10	10.0.1.10	TCP	58	46681 > 4444 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
14	22.869144	10.0.1.10	10.0.0.10	TCP	60	80 > 46681 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
15	22.869234	10.0.0.10	10.0.1.10	TCP	54	46681 > 80 [RST] Seq=1 Win=0 Len=0
16	22.869274	10.0.1.10	10.0.0.10	TCP	60	4444 > 46681 [SYN, AC[illegible] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
17	22.869279	10.0.0.10	10.0.1.10	TCP	54	46681 > 4444 [RST] Se[illegible]=0 Len=0

```
root@ubuntu:~# nmap 10.0.1.10 -Pn -sS -p 80,4444

Starting Nmap 5.21 ( http://nmap.org ) at 2012-07-13 12:23 PDT
Nmap scan report for 10.0.1.10
Host is up (0.00044s latency).
PORT      STATE SERVICE
80/tcp    open  http
4444/tcp open  krb524

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
root@ubuntu:~#
```

SYN, ACK For Closed Port

A better way to address the problem…

Introducing Mook Scanner

- C/C++ using libpcap
- Two types of scans available
  - MSS Option Scanning
  - Connect Response Scanning
- Confidence scoring

MSS Option Scanning

- Essentially a SYN Scan
- Dependent on FW Configuration
- Detect if Host or FW is replying in SYN, ACK response
- Typically FW will set a different MSS Value than the Host
- Ported to Nmap, works kind of… a patch may be available ;)

Process:

1. Send SYN with no MSS Option Set
2. If SYN,ACK MSS Option size is same as user defined size then mark port as open and raise confidence by 1

fishnet SECURITY
Securely Enabling Business

Connect Response Scanning

- Kind of like Nmap connect scan
- Works with all implementations of SYN Flood Protections
- Not sure if it can be ported to Nmap without huge overhaul.

Process:

1. Connect() to complete 3-way handshake
2. Close() socket
3. Listen for ACK; PSH,ACK; or FIN,ACK
4. For each response raise confidence by 1

fishnet SECURITY
Securely Enabling Business

Tempting the Demo Gods…

- Time to see Mook in action!

Come and get some…

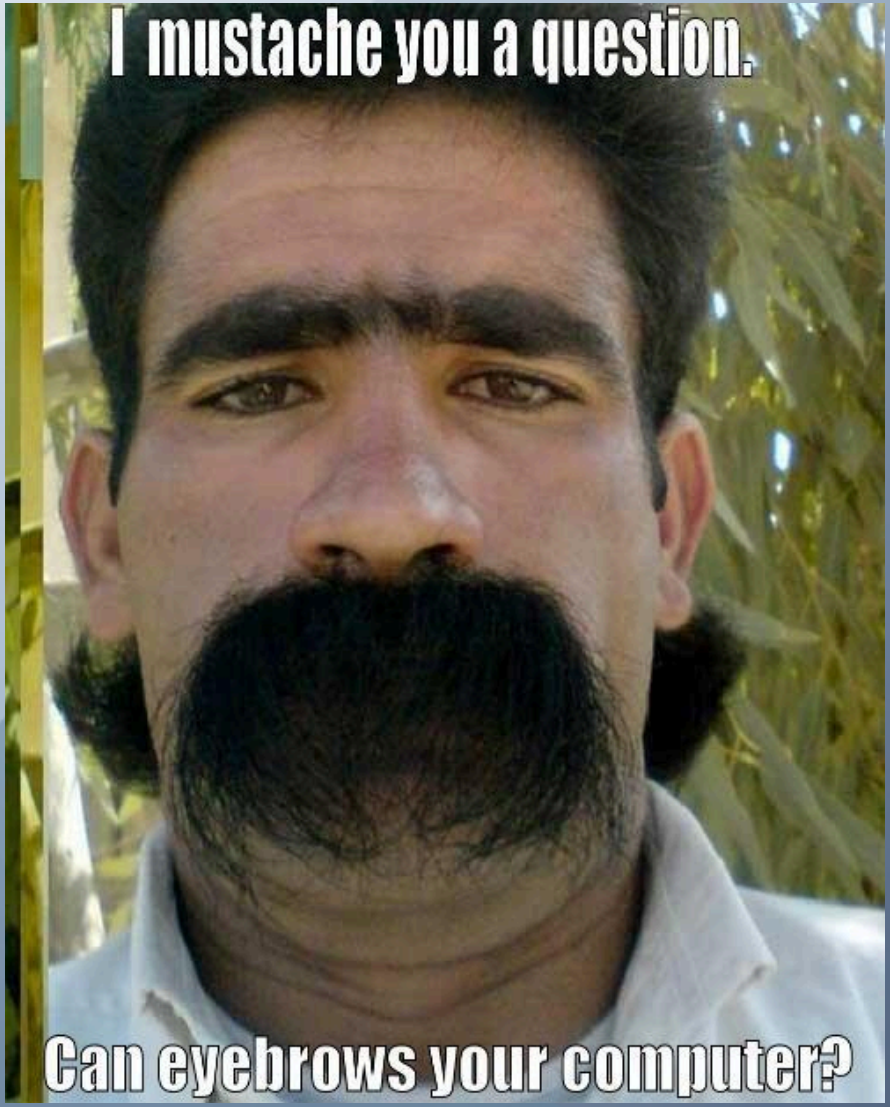
Huptwo34.com: http://huptwo34.com/mook/mook.html

Questions?…

Thank you!

Comments Welcome!

Got Skills…Lets talk!



fishnet SECURITY
Securely Enabling Business

References…

- BSD PF: Synproxy State
- Netfilter/IP Tables: xtables-addons
- F5: SYN Check
- Juniper: SYN Protector
- Cisco: TCP Intercept
- Mook: mook
- FishNet Security: 6labs