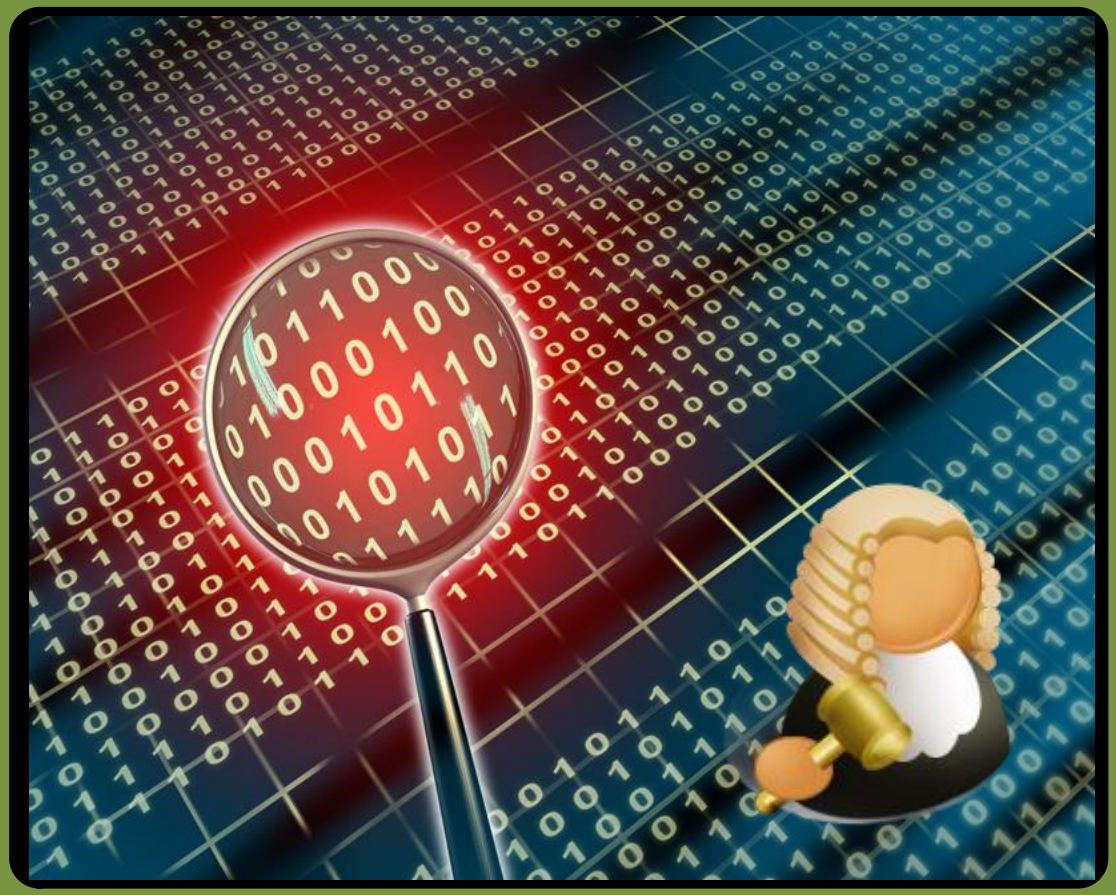
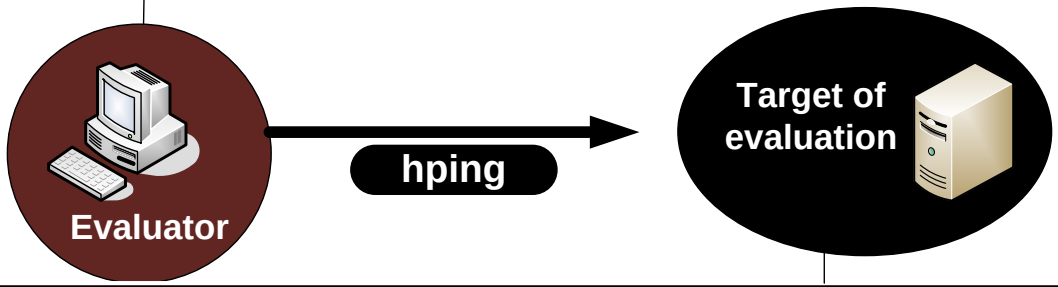
Intrusion Detection



Hping

Author: Prof Bill Buchanan

```
napier@ubuntu:~$ sudo hping -S 192.168.75.132 -e eth0
[sudo] password for napier:
HPING 192.168.75.132 (eth0 192.168.75.132): S set, 40 headers + 4 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=192.168.75.132 ttl=128 id=2052 sport=0 flags=RA seq=0 win=0 rtt=69.3 ms
len=46 ip=192.168.75.132 ttl=128 id=2053 sport=0 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.75.132 ttl=128 id=2054 sport=0 flags=RA seq=2 win=0 rtt=8.9 ms
--- 192.168.75.132 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
```



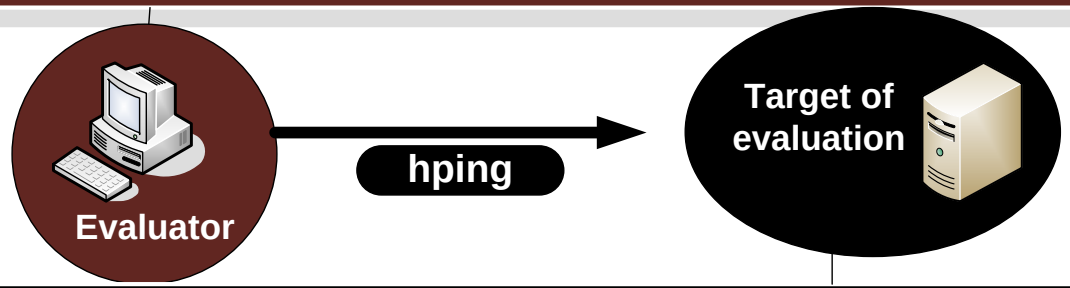

```
14:03:05.859738 IP ubuntu.local.2714 > 192.168.75.132.0: Flags [S], seq
  1222983093:1222983097, win 512, length 4
14:03:05.859975 IP 192.168.75.132.0 > ubuntu.local.2714: Flags [R.], seq 0, ack
  1222983098, win 0, length 0
14:03:06.860566 IP ubuntu.local.2715 > 192.168.75.132.0: Flags [S], seq
  1026211710:1026211714, win 512, length 4
```

Vulnerability

Threats

Author: Prof Bill Buchanan

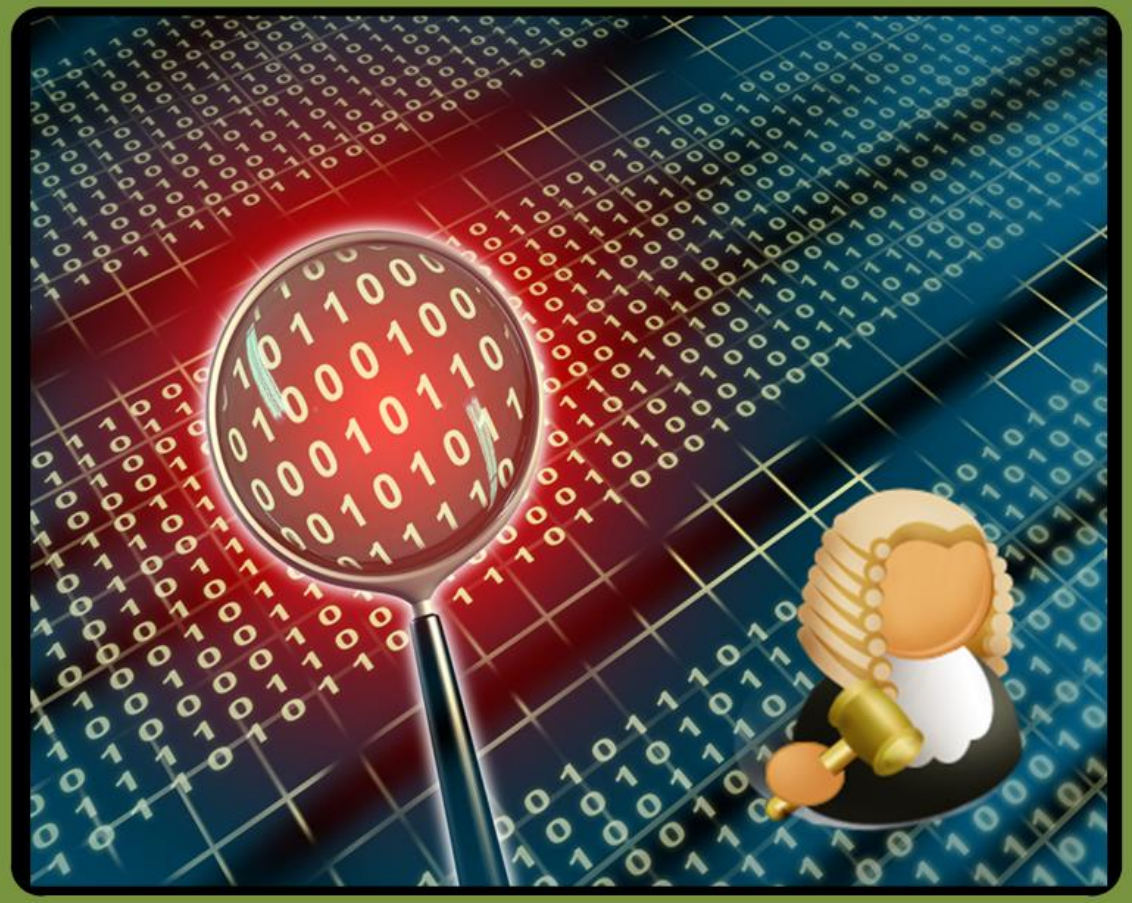
```
napier@ubuntu:~$ sudo hping -S 192.168.75.132 -e eth0 -p 80
HPING 192.168.75.132 (eth0 192.168.75.132): S set, 40 headers + 4 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=192.168.75.132 ttl=128 id=2072 sport=80 flags=SA seq=0 win=64240 rtt=11.3
ms
len=46 ip=192.168.75.132 ttl=128 id=2073 sport=80 flags=SA seq=1 win=64240 rtt=0.5
ms
len=46 ip=192.168.75.132 ttl=128 id=2074 sport=80 flags=SA seq=2 win=64240 rtt=0.4
ms
--- 192.168.75.132 hping statistic ---
15 packets transmitted, 15 packets received, 0% packet loss
round-trip min/avg/max = 0.4/1.5/11.3 ms
```




```
14:04:31.090418 IP ubuntu.local.2222 > 192.168.75.132.www: Flags [S], seq
  56776272:56776276, win 512, length 4
14:04:31.092037 IP ubuntu.local.57490 > 192.168.75.2.domain: 34223+ PTR?
  132.75.168.192.in-addr.arpa. (45)
14:04:31.093064 IP 192.168.75.132.www > ubuntu.local.2222: Flags [S.], seq
  447090437, ack 56776273, win 64240, options [mss 1460], length 0
14:04:31.093132 IP ubuntu.local.2222 > 192.168.75.132.www: Flags [R], seq
  56776273, win 0, length 0
```


Author: Prof Bill Buchanan

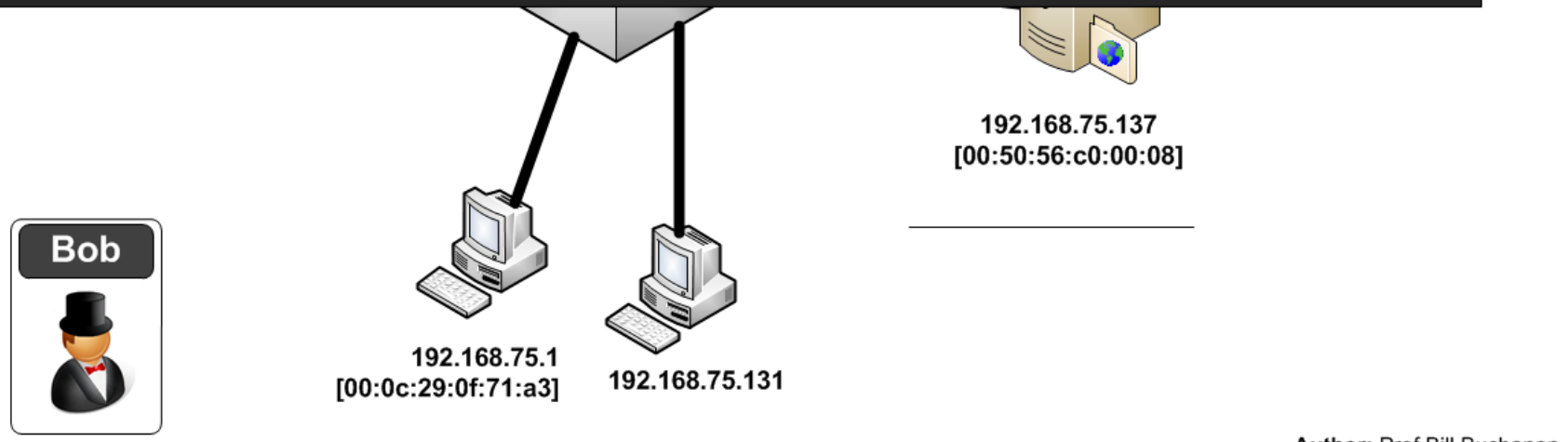
Net Forensics



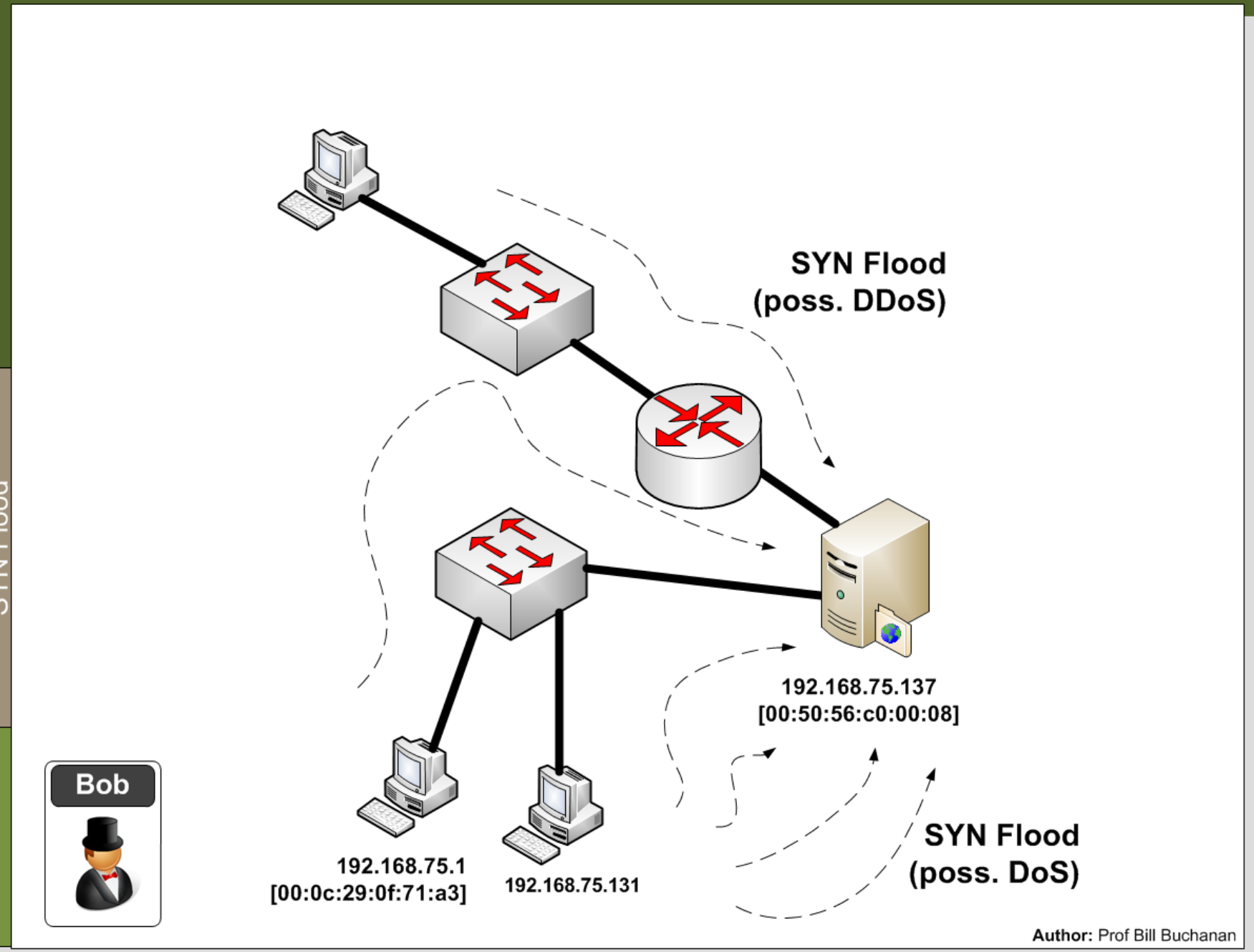
SYN FLOOD

Author: Prof Bill Buchanan

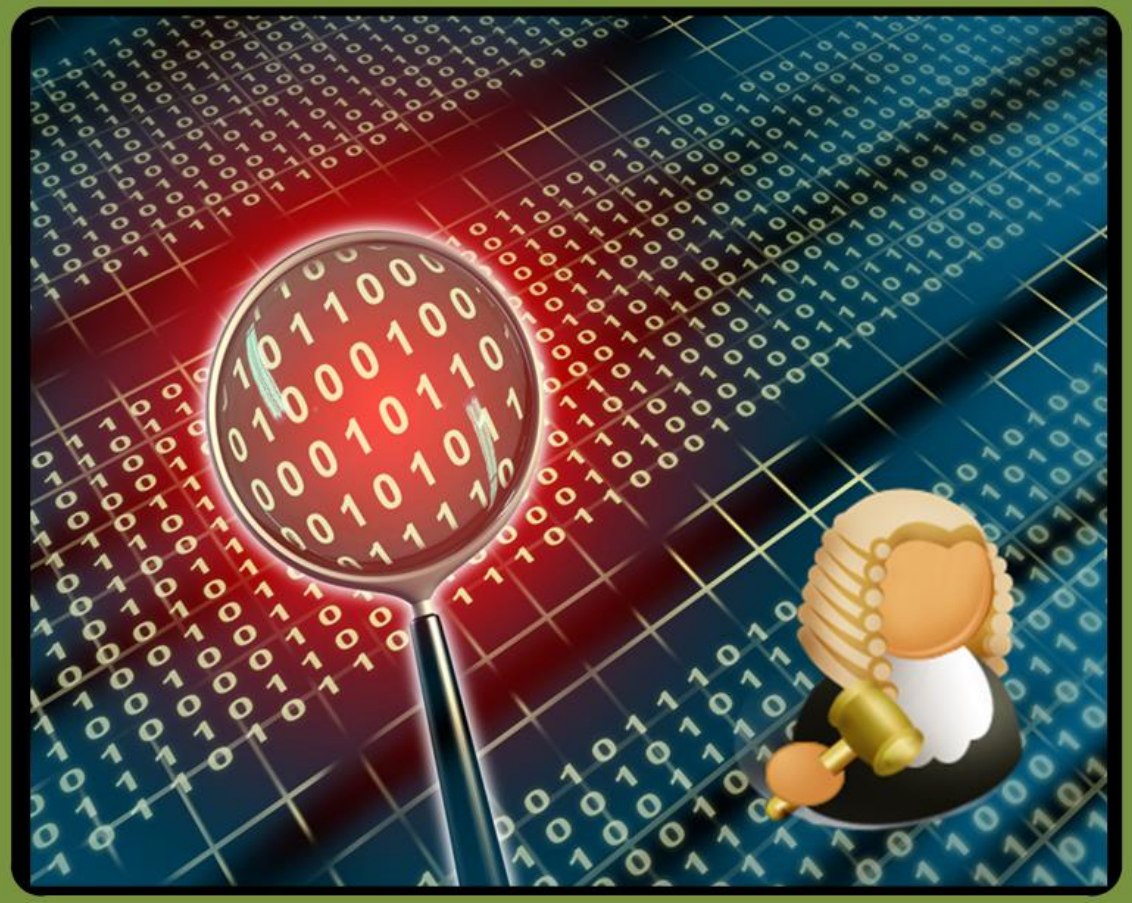
```
No.     Time        Source                Destination           Protocol Info
      2 4.510329    192.168.75.137        192.168.75.1          HTTP     Continuation
or non-HTTP traffic

Frame 2 (58 bytes on wire, 58 bytes captured)
Internet Protocol, Src: 192.168.75.137 (192.168.75.137), Dst: 192.168.75.1
(192.168.75.1)
Transmission Control Protocol, Src Port: smart-lm (1608), Dst Port: http (80), Seq: 0,
Len: 4
Hypertext Transfer Protocol

No.     Time        Source                Destination           Protocol Info
      3 5.514164    192.168.75.137        192.168.75.1          HTTP     Continuation
or non-HTTP traffic

Frame 3 (58 bytes on wire, 58 bytes captured)
Internet Protocol, Src: 192.168.75.137 (192.168.75.137), Dst: 192.168.75.1
(192.168.75.1)
Transmission Control Protocol, Src Port: isysg-lm (1609), Dst Port: http (80), Seq: 0,
Len: 4
Hypertext Transfer Protocol
```



SYN Flood

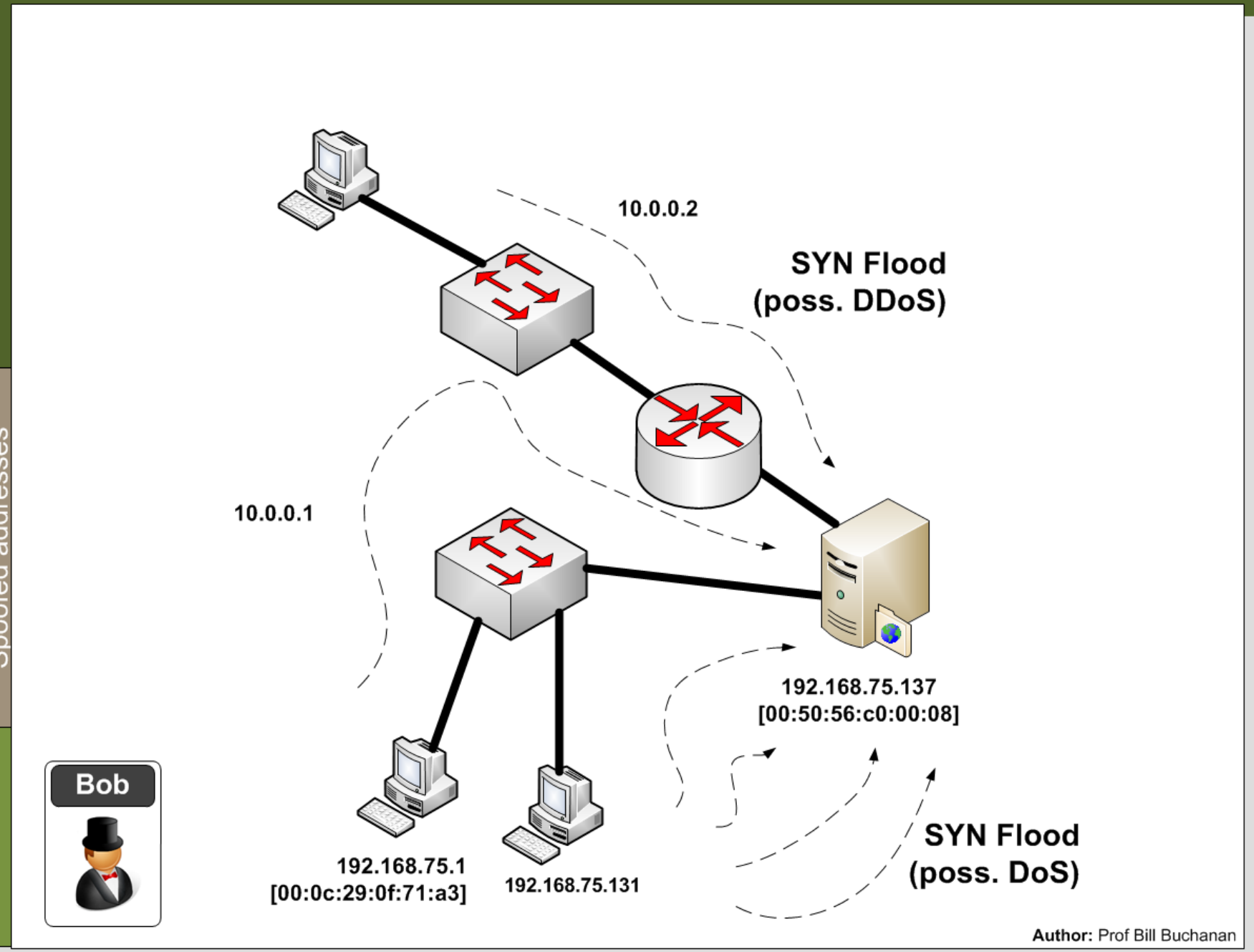

SYN Flood
(poss. DDoS)
192.168.75.137
[00:50:56:c0:00:08]
Bob
192.168.75.1
[00:0c:29:0f:71:a3]
192.168.75.131
SYN Flood
(poss. DoS)
Author: Prof Bill Buchanan

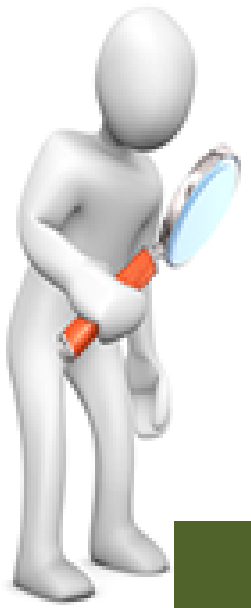
Net Forensics



SPOOFED ADDRESSES

Author: Prof Bill Buchanan


Spoofed addresses
Net Forensics
10.0.0.2
SYN Flood
(poss. DDoS)
10.0.0.1
192.168.75.137
[00:50:56:c0:00:08]
Bob
192.168.75.1
[00:0c:29:0f:71:a3]
192.168.75.131
SYN Flood
(poss. DoS)
Author: Prof Bill Buchanan



Digital

Investigator

Network Intrusions

NMAP and HPING