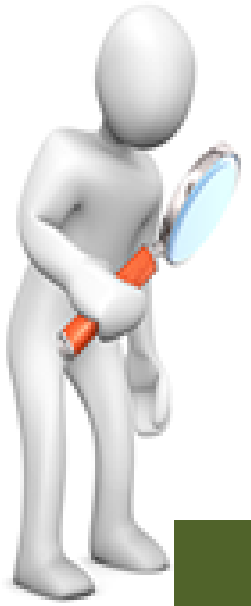


Digital

Investigator

Network Intrusions

Intro to Pen Testing: NMAP and HPING

Intrusion Detection

Introduction to Pen Testing

- Intro to Pen Testing
- Port Scan
- SYN Flood
- Spoofed Address

Author: Prof Bill Buchanan

Pen. Testing

Threats

Good...

... Bad

White Hat

Blue Hat

Grey Hat

Black Hat

Cracker

motivated by financial gain, and has criminal intent

Script kiddies

does not have many skills, and use standard scripting tools

Software Cracker

reverse engineer software applications

Phreakers

hacks telephone systems

Hacktvist

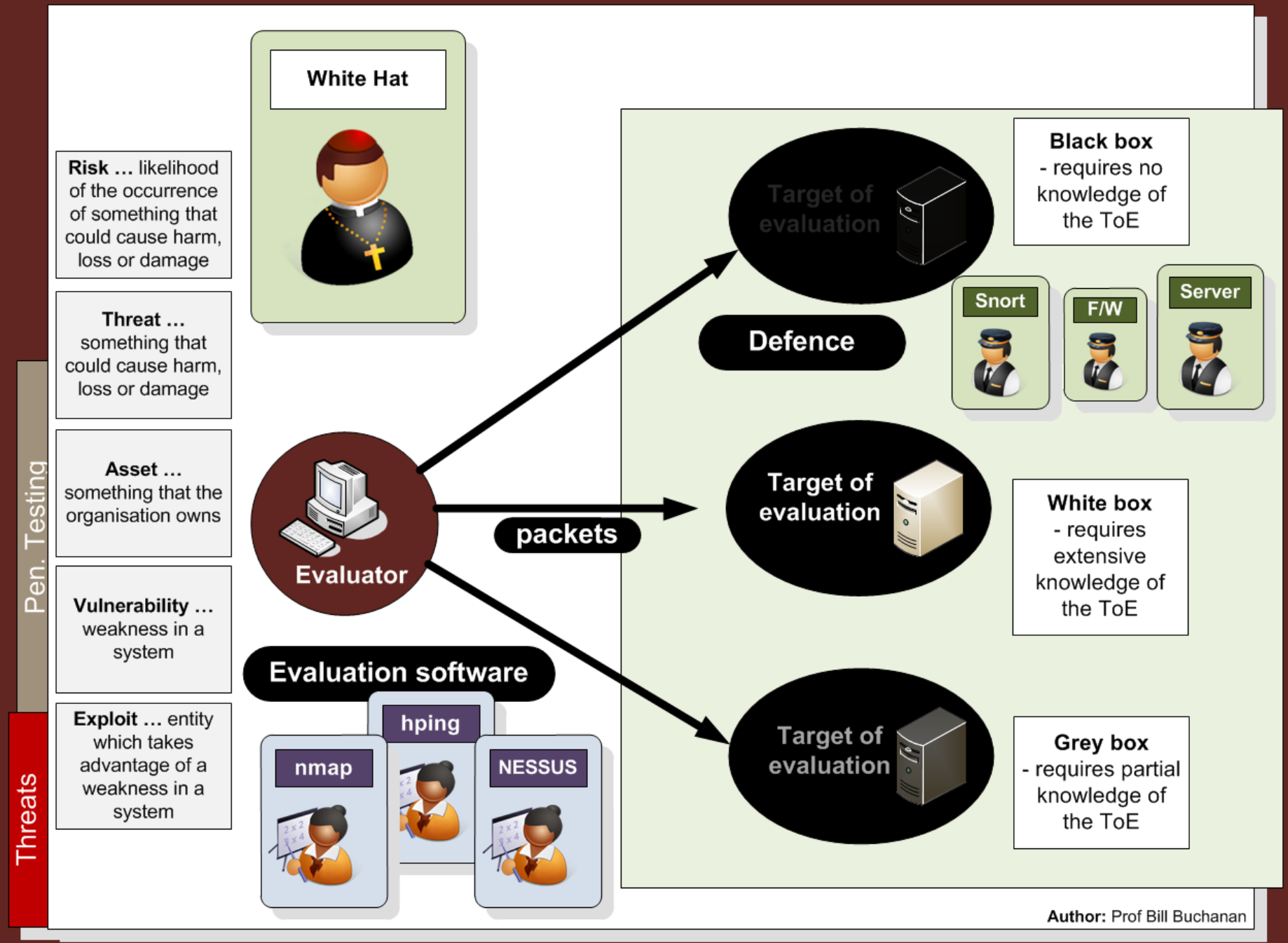
has a political agenda

Whacker

focuses on wireless LAN and WANs

Author: Prof Bill Buchanan

Good and bad



White, grey and black box testing

Code of Ethics

- Do not exceed authorization limits
- Be ethical
- Limit possible damage
- Maintain confidentiality

White Hat

Stolen equipment attack

Social engineering

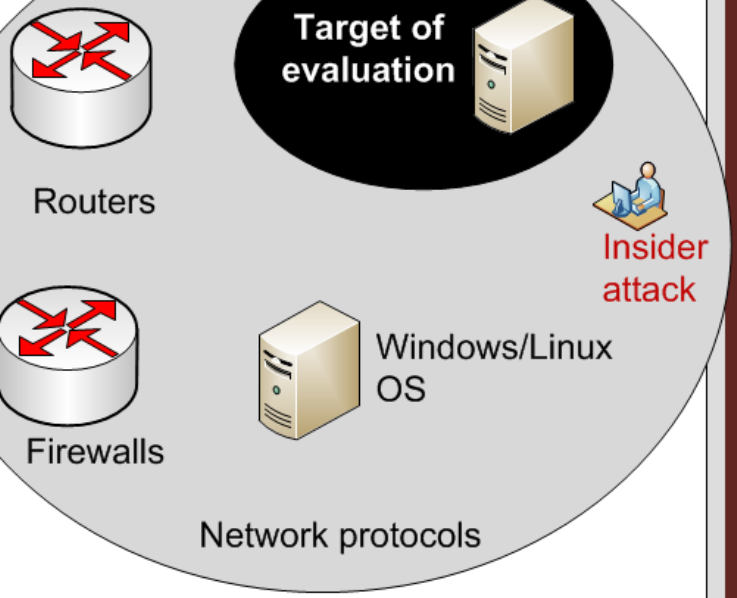
Pen. Testing

Threats

Level I

High-level testing – does not include a hands-on test

Physical entry attack



Level II

Network Evaluation - information gathering, scanning and vulnerability assessment scanning

Level III

Pen Testing - taking on an adversarial role

Outsider attack

Author: Prof Bill Buchanan

Levels of testing

Confidentiality

- Only authorized entities can access sensitive data

Locked doors
Armed guards
Fences
Firewalls
Passwords
Encryption
VPN Access

Access control
Windows File Protection
MD5 checksum
SHA-1 checksum
Network Operating System

Integrity

- Changes data by unauthorized entities is detected.
- Only authorized entities can change sensitive data

Target of evaluation

Availability

- Only authorized entities have continual access to data

Failover equipment
Mirror servers

Pen. Testing

Threats

Author: Prof Bill Buchanan

CIA

Code of Ethics

- Do not exceed authorization limits
- Be ethical
- Limit possible damage
- Maintain confidentiality

White Hat

Pen. Testing

Threats

Written permission from the organisation.

Scope the project

Perform the assessment

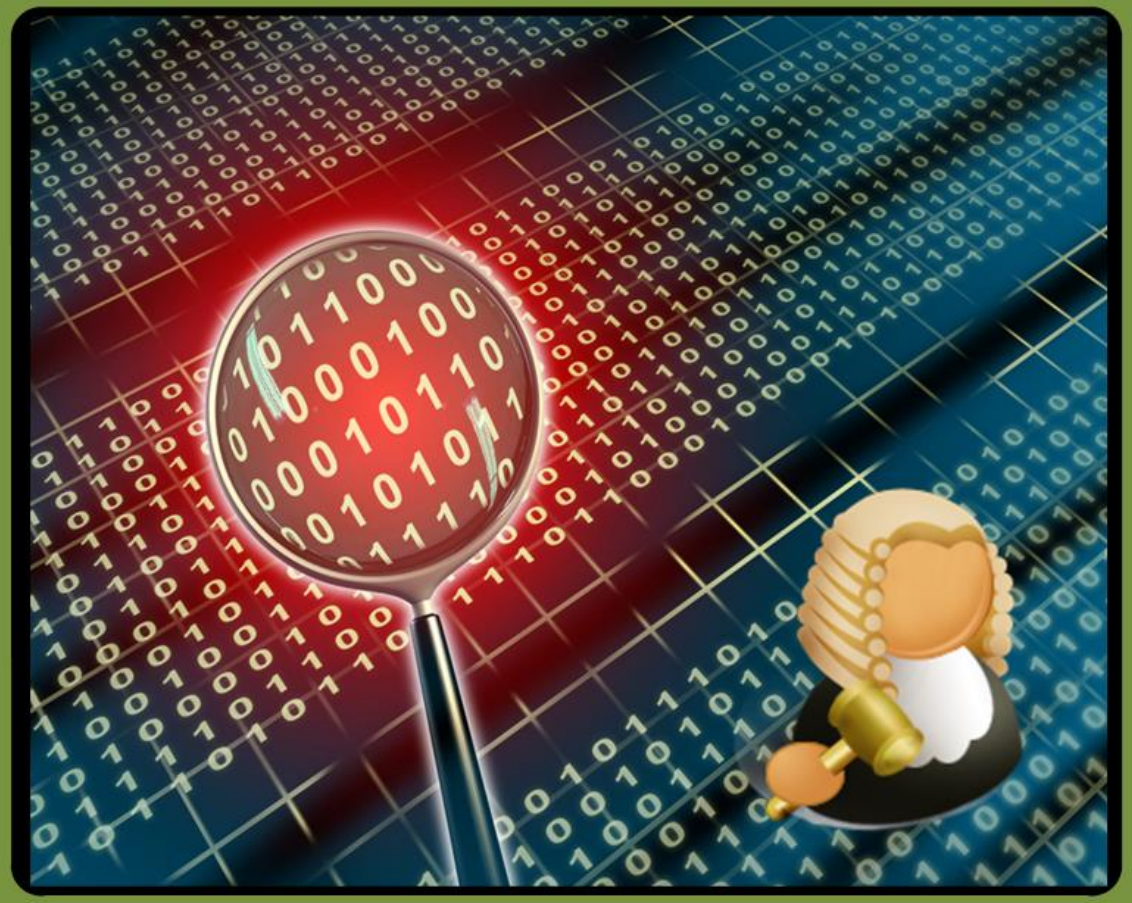
Post assessment activities

Why?

- **Gramm-Leach-Bliley Act** (US reg to allow banks, security firms and insurance companies to merge/share data)
- **US Health Insurance Portability and Accountability Act (HIPAA)**.
- **Security and Freedom through Encryption (SAFE)**. define the rights of US Citizens to the use of encryption without key escrow.
- **Computer Fraud and Abuse Act**. Reduce hacking by defining penalties against incidents.
- **Privacy Act of 1974**. Respects the rights of the individual unless permission is given.
- **Federal Information Security Management Act (FISMA)**. Aims to strengthen US federal government security by the use of yearly audits.
- **Economic Espionage Act of 1996**. Aims to criminalise the misuse of trade secrets.
- **Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT)**. Permits the government to monitor hackers without a warrant.
- **Sarbanes-Oxley (SOX) Act**. Relates to transparent account and reporting of companies

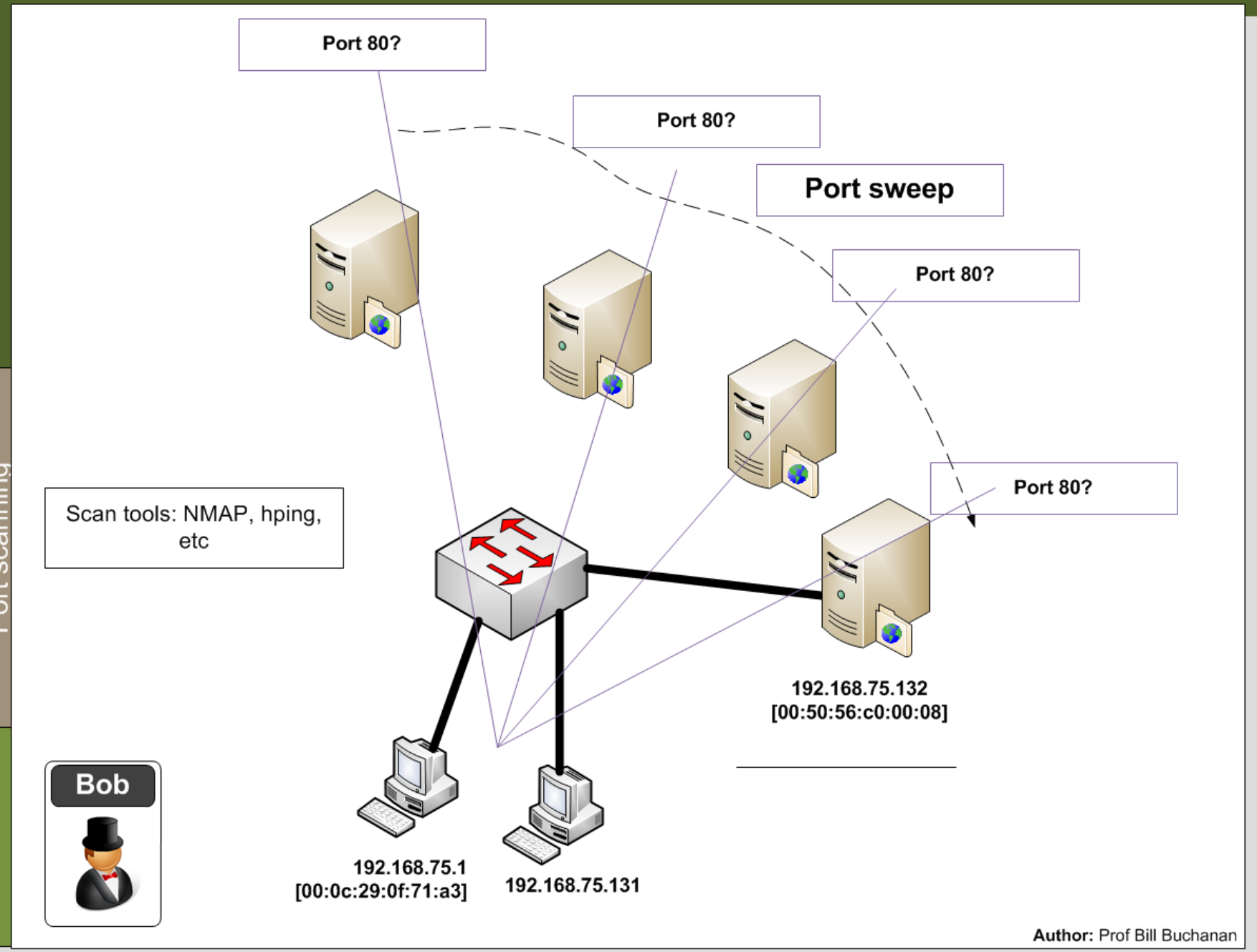
Author: Prof Bill Buchanan

Net Forensics



Port Scan

Author: Prof Bill Buchanan

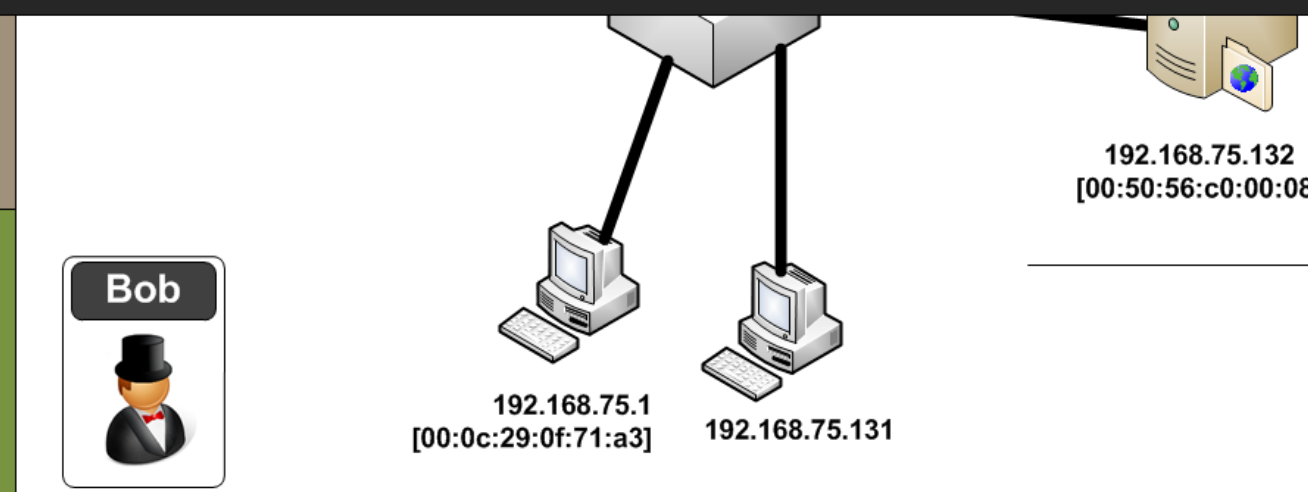


Port scanning

Net Forensics

Port sweep

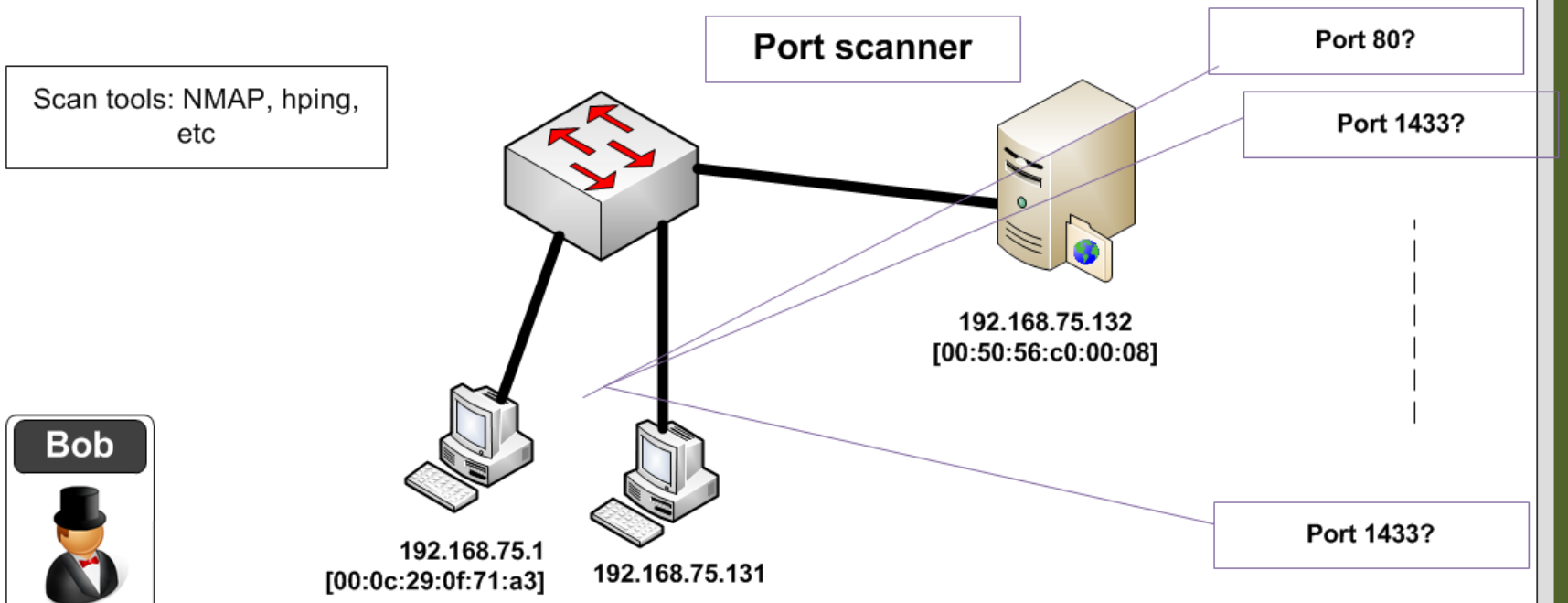
```
No.     Time        Source                Destination           Protocol Info
     85 25.420710   192.168.75.1          192.168.75.132        TCP      54370 > telnet
[SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 85 (58 bytes on wire, 58 bytes captured)
Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132
(192.168.75.132)
Transmission Control Protocol, Src Port: 54370 (54370), Dst Port: telnet (23), Seq: 0,
Len: 0

No.     Time        Source                Destination           Protocol Info
     86 25.420836   192.168.75.1          192.168.75.132        TCP      54370 > rap
[SYN] Seq=0 Win=2048 Len=0 MSS=1460

Frame 86 (58 bytes on wire, 58 bytes captured)
Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132
(192.168.75.132)
Transmission Control Protocol, Src Port: 54370 (54370), Dst Port: rap (256), Seq: 0,
Len: 0
```



Port Scan

TCP Scan	SYN	SYN/ACK	ACK	FIN/ACK
SYN Scan	SYN		Creates half-open connections	
FIN Scan	FIN		Closed ports respond with a RST, but open ports ignore.	

Scan tools: NMAP, hping, etc



Author: Prof Bill Buchanan

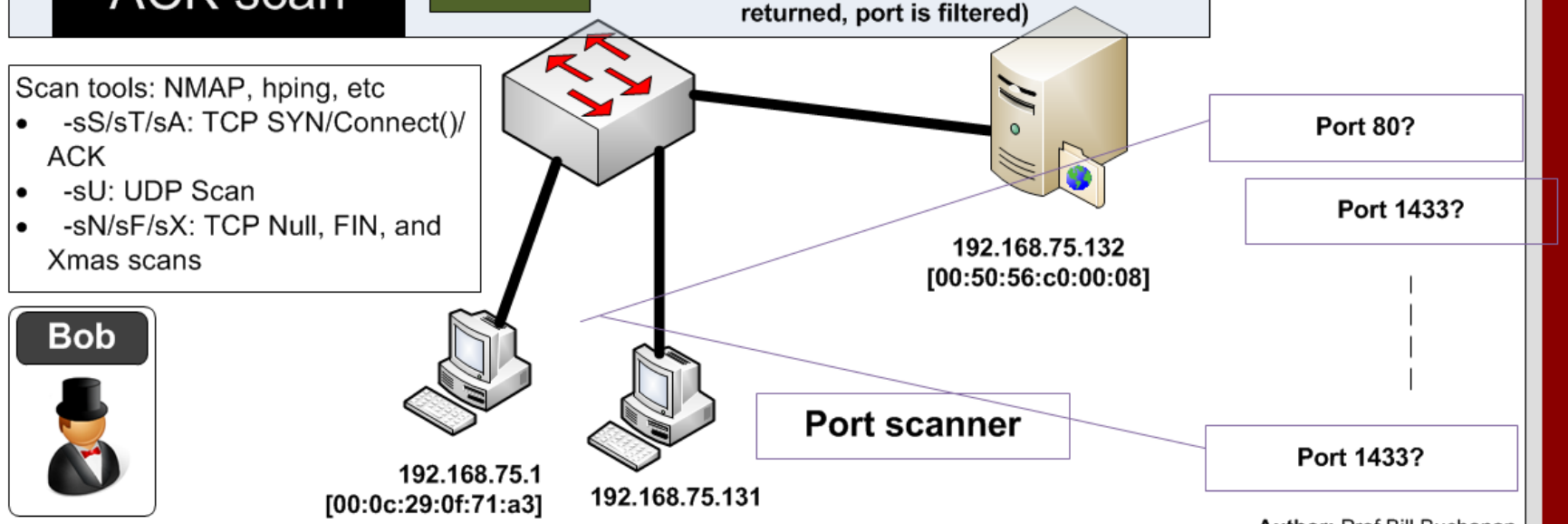
Port scanning

CEH

Connect Scan	SYN	ACK	FIN/ACK	Open ports: SYN/ACK; Closed ports: RST/ACK
SYN Scan	SYN			Creates half-open connections
FIN Scan	FIN			Closed ports respond with a RST, but open ports ignore.
NULL scan				Open ports; Closed ports: RST
XMAS scan	FIN	URG	PSH	
ACK scan	ACK			Determines ACLs on firewall or if stateless inspection (if ICMP Destination Unreachable returned, port is filtered)

Scan tools: NMAP, hping, etc

- -sS/sT/sA: TCP SYN/Connect()/ ACK
- -sU: UDP Scan
- -sN/sF/sX: TCP Null, FIN, and Xmas scans



Author: Prof Bill Buchanan

Port scan