

https://xkcd.com/1421/

CS 60:
Computer Networks

Pen testing; IDS/IPS; scanning

Review from last class

A firewall acts as a barrier between a trusted network and the rest of the malicious Internet

Firewalls can be software (often protect a single host) or a hardware appliance (often protect a network)

Four types of firewalls

1. Packet filters (or stateless firewalls)
2. Stateful firewalls
3. Application proxies
4. Next Generation

Make sure you can write simple iptables rules

See examples at end of deck from last class

In Linux we can write our own firewall rules

- Loadable Kernel Modules (LKMs)
- iptables

Agenda



1. Penetration testing
2. Network scanning
3. IDS/IPS
4. Incident response planning
5. Economics
6. Certifications

Discussion

What can an organization say about whether it has been compromised?

If an organization has been compromised, are the security people who work there lazy/incompetent/only care about money?

What is a penetration test, why run one?

What should you test?

- People
- Process
- Technology

Testing comes in several flavors







Audits

- Check documentation
- Review disaster recovery and incident response plans, security policies
- Often done as part of due diligence

Vulnerability scans

- Look for known vulnerabilities in systems
- Check against Common Vulnerabilities and Exposures (CVE)

Penetration tests

- Try to exploit people, process, and technology
- Simulate an adversary trying to gain access
- Fix problems before exploited

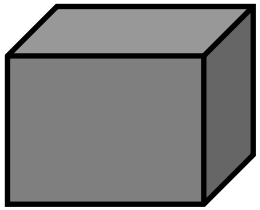
Easttom II, William Chuck. *Penetration testing fundamentals: A hands-on guide to reliable security audits*. Pearson IT Certification, 2018.

A penetration test simulates an attack on a system

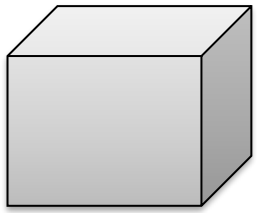
Vulnerability assessments look for known weaknesses but do not try to exploit them

Penetration tests (aka ethical hacking, white hat hacking) try to gain access and escalate privileges

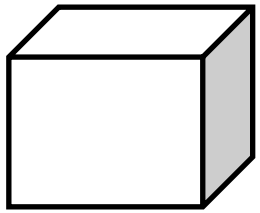
Risks?
What if the test breaks/DoS's your production systems?



Closed box
Testers given no knowledge of network



Grey box
Testers given some knowledge of network



Open box
Testers given complete knowledge of network

Goal: find and fix problems before they are exploited by adversaries

You're safe if the penetration test can't get access, right? I've talked with people who say they have never found a network they can't get into. What about AI swarms?

Pen Test Execution Standard (PTES) recommends seven stages in a pen test

Pre-engagement interactions

- Define scope/expectations (some systems may be excluded)
- Create clear contract

Agree on what will be tested, when

Intelligence gathering

- OSINT
- Other intel (may be client provided)

Get out of jail free card for testers!

Threat modelling

- Contemplate threats (APT, script kiddies)
- Model their likely approach

Vulnerability analysis

- Run vulnerability scanners to find targets to exploit
- Metasploit, Nmap, Nessus, Zap, Burp Suite, custom tools

Exploitation

- Attempt to breach target
- Look for network responses/defensive actions

Post exploitation

- Attempt to escalate privileges
- Install backdoors

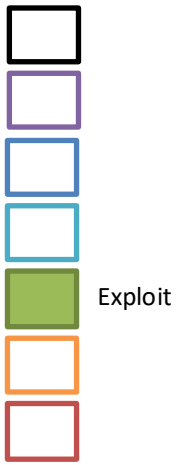
Reporting

- Report findings of penetration test
- Recommend remediation steps

http://www.pentest-standard.org/index.php/Main_Page

The exploitation phase is often broken into four steps

Exploitation phase steps



1. **Passive scanning**
   - Gather as much data on target as possible
   - Sniffing, OSINT, and maybe *social engineering*
   - Risk of detection is low

What is social engineering?

2. **Active scanning**
   - Scan ports on all available IP addresses (nmap)
   - Run vulnerability scanners (nmap, Nessus, ZAP, Metasploit)
   - Risk of detection increased
3. **Breaching**
   - Manually conducting exploits (buffer overflows, SQL attacks, XSS)
   - Phishing
   - Metasploit/benign payloads

Conducted by "red team" or "OPFOR"

4. **Completion**
   - Fix holes

Adapted from Easttom II, William Chuck. *Penetration testing fundamentals: A hands-on guide to reliable security audits*. Pearson IT Certification, 2018.

Pen tests are often conducted in two phases: external then internal

1) External: test from outside

- Port scan public-facing IP addresses (e.g., web server, gateway router)
- Identify OS and service versions
- Try default passwords
- Use vulnerability scanners on discovered devices (nmap, ZAP, Burp Suite)
- Manually attempt common attacks (XSS, SQL injection, etc)
- Try Metasploit
- Attempt wireless access (try to get admin on Wi-Fi router)
- Phishing emails/social engineering



2) Internal: test from inside

- Perform external steps but from inside
- Use sniffer to look for passwords/encrypted data
- Covert entry/physical security
- Bug sweeps

I used to do external test as closed box and internal tests as open box

Discussion

After the test is done, how to prioritize what to fix first?

After my first penetration test, presenting results to the board of directors

- Me to pen testers before presenting findings:
  - We are presenting to the non-technical board
  - Give them the high-level picture of where we stand
  - Unless they ask, don't get into a discussion of specific bugs
- Pen testers presenting to the board:
  - First thing: Let me tell you about the Unix R-login bug because it is really interesting…
- Board to me:
  - What does this mean?
  - How are we doing?
  - What do we do next?

So how do you present the findings to the non-technical board?

What does the board really want to know?

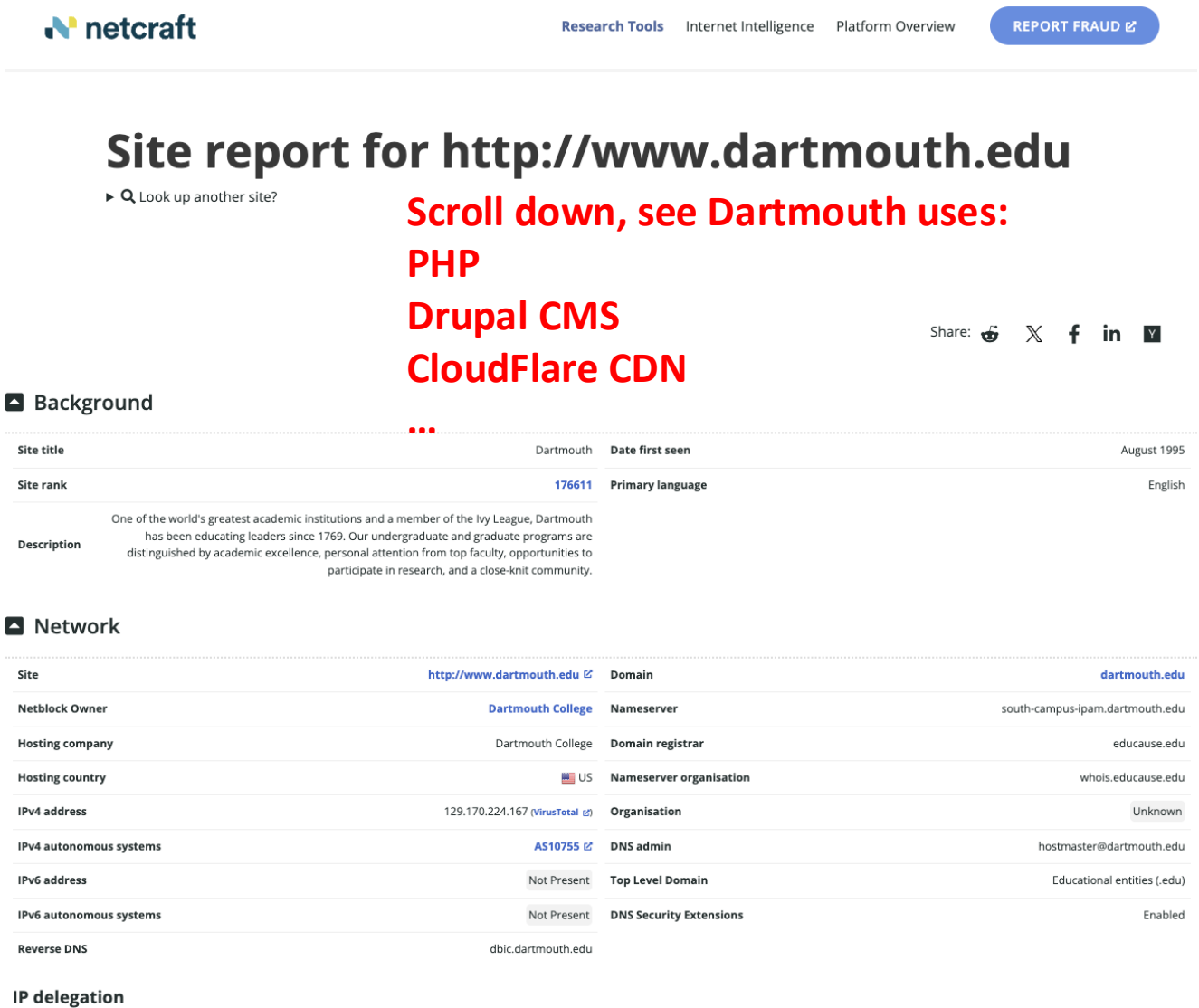
They want to know you have a plan to address issues and will follow up with them when you are done

Agenda

1. Penetration testing
2. Network scanning
3. IDS/IPS
4. Incident response planning
5. Economics
6. Certifications

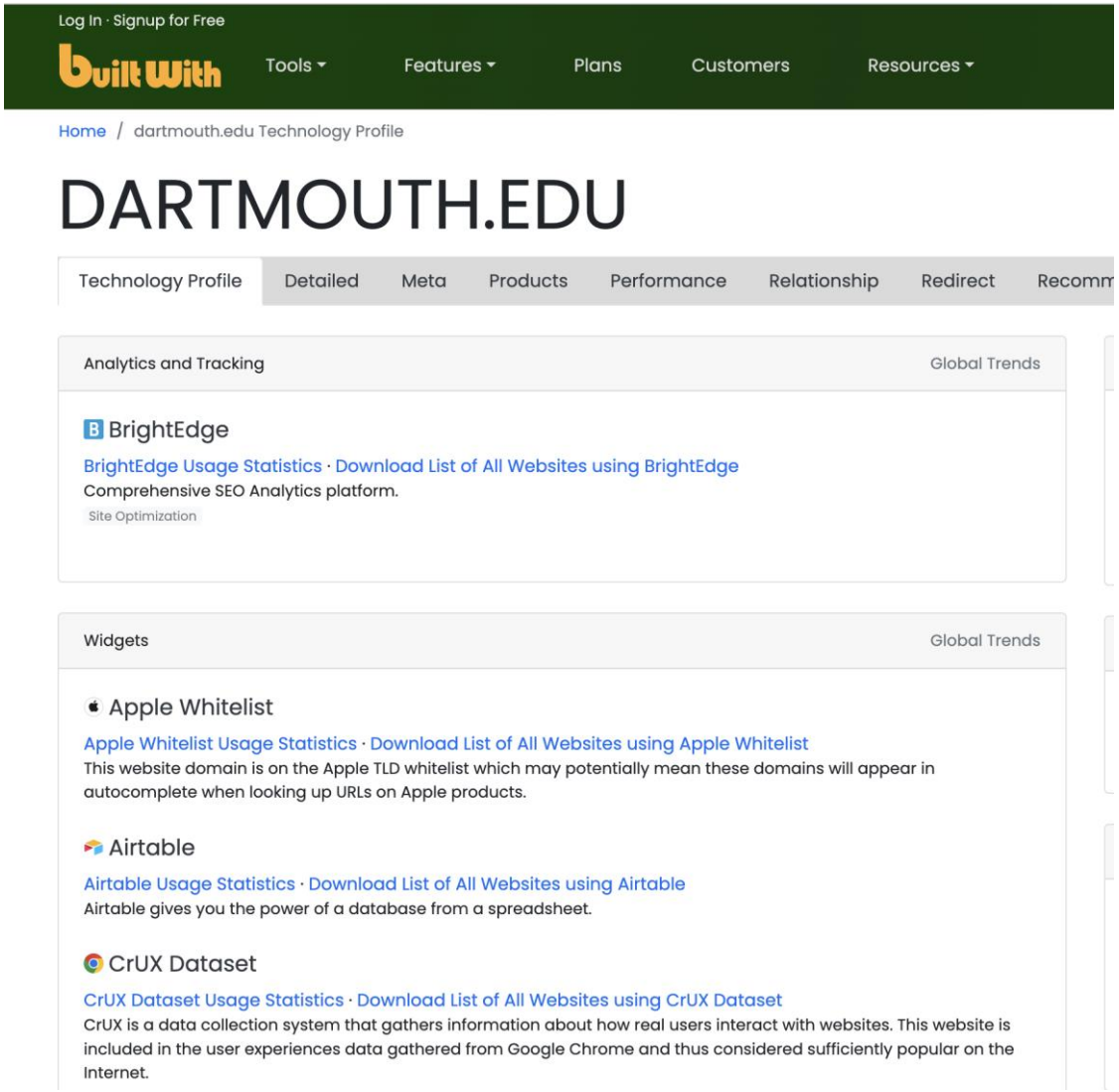
Passive techniques can reveal a lot about a target, start with netcraft.com

www.netcraft.com



Check out builtwith.com to passively learn about technologies used by organization

www.builtwith.com



Builtwith and Netcraft scan organizations and present findings

You can sometimes learn a lot without ever sending a packet to a target network

Shodan.io scans the Internet for vulnerable devices

www.shodan.io

net: <subnet mask> to find vulnerable devices



TOTAL RESULTS

10

TOP PORTS

80	5
443	4
548	1

TOP ORGANIZATIONS

Amazon Technologies Inc.	4
Amazon Data Services Northern Virginia	3
Dartmouth College	2
Amazon.com, Inc.	1

View Report | View on Map | Advanced Search

Product Spotlight: A native desktop app to access Shodan using your API key. Fast and optimized for power users. Check out Shodan Terminal.

98.95.252.212

dartmouth.edu
ec2-98-95-252-212.compute-1.amazonaws.com
Amazon Data Services Northern Virginia
United States, Ashburn
cloud

SSL Certificate
Issued By:
|- Common Name:
InCommon Intermediate CA - OVG2C
|- Organization:
Internet2
Issued To:
|- Common Name:
***.dartmouth.edu**
|- Organization:
Dartmouth College
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 302 Found
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Date: Wed, 04 Nov 2026 12:37:10 GMT
Location: https://login.microsoftonline.com/995b0936-48d6-40e5-a31e-bf689ec9446f/oauth2/v2
```

98.95.252.212

ec2-98-95-252-212.compute-1.amazonaws.com
Amazon Data Services Northern Virginia
United States, Ashburn
cloud

```
HTTP/1.1 302 Found
Cache-Control: no-store
Content-Type: text/html; charset=utf-8
Date: Wed, 04 Nov 2026 12:12:01 GMT
Location: https://login.microsoftonline.com/995b0936-48d6-40e5-a31e-bf689ec9446f/oauth2/v2.0/authorize?client_id=1f78610
```

3.224.254.200

Devices are often left with default usernames and passwords

	Router Brand	Default IP Address	Default Username	Default Password
1	3Com	http://192.168.1.1	admin	Admin
2	Belkin	http://192.168.2.1	admin	admin
3	BenQ	http://192.168.1.1	admin	Admin
4	D-Link	http://192.168.0.1	admin	Admin
5	Digicom	http://192.168.1.254	admin	Michelangelo
6	Linksys	http://192.168.1.1	admin	Admin
7	Netgear	http://192.168.0.1	admin	password
8	Sitecom	http://192.168.0.1	sitecom	Admin
9	Asus	http://192.168.1.1	admin	admin
10	Synology	http://192.168.1.1	admin	Admin
11	Arris	http://192.168.0.1	admin	password
12	Apple iphoneIOS4.X	http://10.0.1.1	root	alpine
13	DELL	http://192.168.1.1	admin	password
14	Huawei ADSL2+	http://192.168.0.1	admin	admin
15	Netcomm	http://192.168.1.1	admin	password
16	Netstar	http://192.168.0.1	admin	password
17	SAMSUNG	http://192.168.0.1	admin	password

https://www.softwaretestinghelp.com/default-router-username-and-password-list/

Can also check the device's user manual to find default credentials

Mirai botnet compromised thousands of webcams using default credentials; took down DNS

Make sure you change default passwords!

Adversaries try to learn about the network without alerting people to their presence

Network scanning methodology

Nmap is an amazingly powerful tool that can help with these steps

1. **Check for live systems**
   - Gives a list of computers are on the network
   - Ping can do this
2. **Check for open ports**
   - Different machines will run different services
   - Services typically run using standard ports (e.g., ssh on port 22)
   - See ports on which computers are listening
3. **Scan around the IDS**
   - Don't be too noisy, avoid IDS detection
4. **Perform banner grabbing**
   - Finds OS and versions services are running
5. **Scan for vulnerabilities**
   - Given OS and service versions, check CVE
6. **Draw network diagrams**

Walker, Matt. *CEH Certified Ethical Hacker All-In-One Study Guide, Fourth Edition*. McGraw-Hill, 2019.

A pen tester (or adversary) may try to actively discover computers on a network

```
# Ping can tell you if a device is up
$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.880 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.668 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.577 ms
```

Must know device's IP address
Could manually try pinging each device in an IP range
$ ping 10.0.2.1
$ ping 10.0.2.2
$ ping 10.0.2.3
…
A network of 10.0.2.0/24 could have 254 hosts (0 and 255 are reserved)
Tedious to do by hand!
Can you script it?
Lab5 says yes!

This section is inspired by NetworkChuck: https://www.youtube.com/watch?v=4t4kBkMsDbQ

Step 1: check for live systems

nmap can quickly ping all devices on a network

$ nmap –sP 10.0.2.0/24

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-05-05 14:07 EST
Nmap scan report for 10.0.2.1
Host is up (0.0015s latency).
Nmap scan report for 10.0.2.2
Host is up (0.0013s latency).
Nmap scan report for 10.0.2.5
Host is up (0.00067s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00057s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.55 seconds
```

Us

Pings all devices on a network

Not many devices up on the VM's network

But now we know which IP address are in use

Interesting target?

Many services run on well-known ports

Port Number	Protocol	Transport Protocol	Port Number	Protocol	Transport Protocol
20/21	FTP	TCP	110	POP3	TCP
22	SSH	TCP	135	RPC	TCP
23	Telnet	TCP	137–139	NetBIOS	TCP and UDP
25	SMTP	TCP	143	IMAP	TCP
53	DNS	TCP and UDP	161/162	SNMP	UDP
67	DHCP	UDP	389	LDAP	TCP and UDP
69	TFTP	UDP	443	HTTPS	TCP
80	HTTP	TCP	445	SMB	TCP

Walker, Matt. *CEH Certified Ethical Hacker All-In-One Study Guide, Fourth Edition*. McGraw-Hill, 2019.

Step 2: check for open ports

nmap can find all open ports on a particular computer

$ nmap -sT 10.0.2.15

Starting Nmap 7.01 (https://nmap.org) at 2021-05-05 14:48 EST
Nmap scan report for 10.0.2.15
Host is up (0.00098s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
53/tcp open domain
80/tcp open http
3128/tcp open squid-http

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

Uses TCP to check for open ports
Running web server (among others)
Squid is a web proxy (suggests web server is operating)

Step 2: check for open ports

nmap can find all open ports on a particular computer

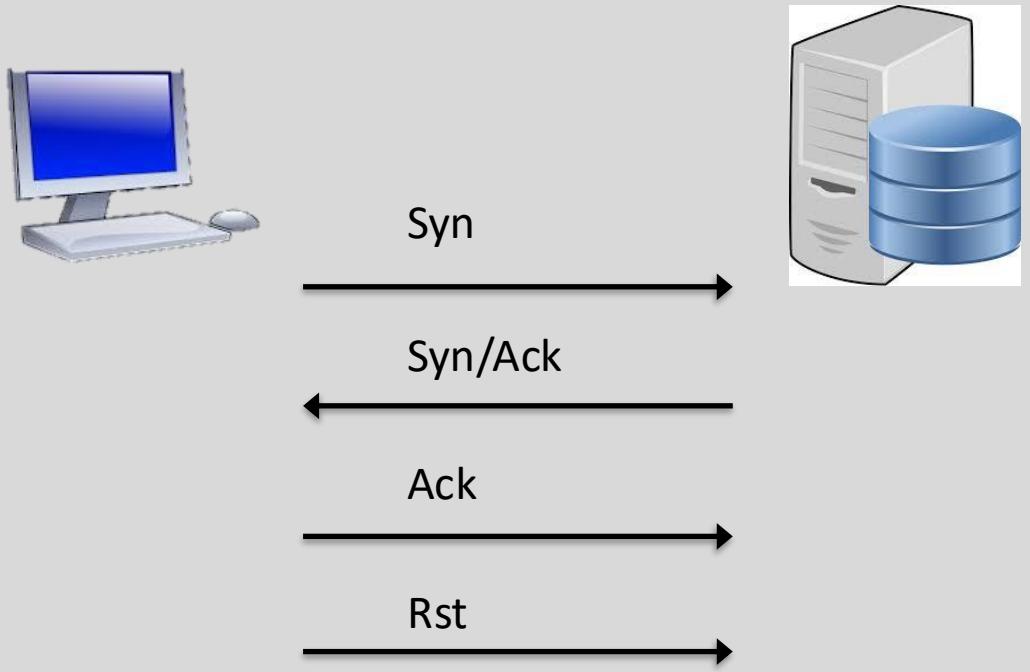
$ nmap -sT 10.0.2.15

This command uses the whole 3-way handshake (full-open scan)

Noisy, IDS might detect this much activity

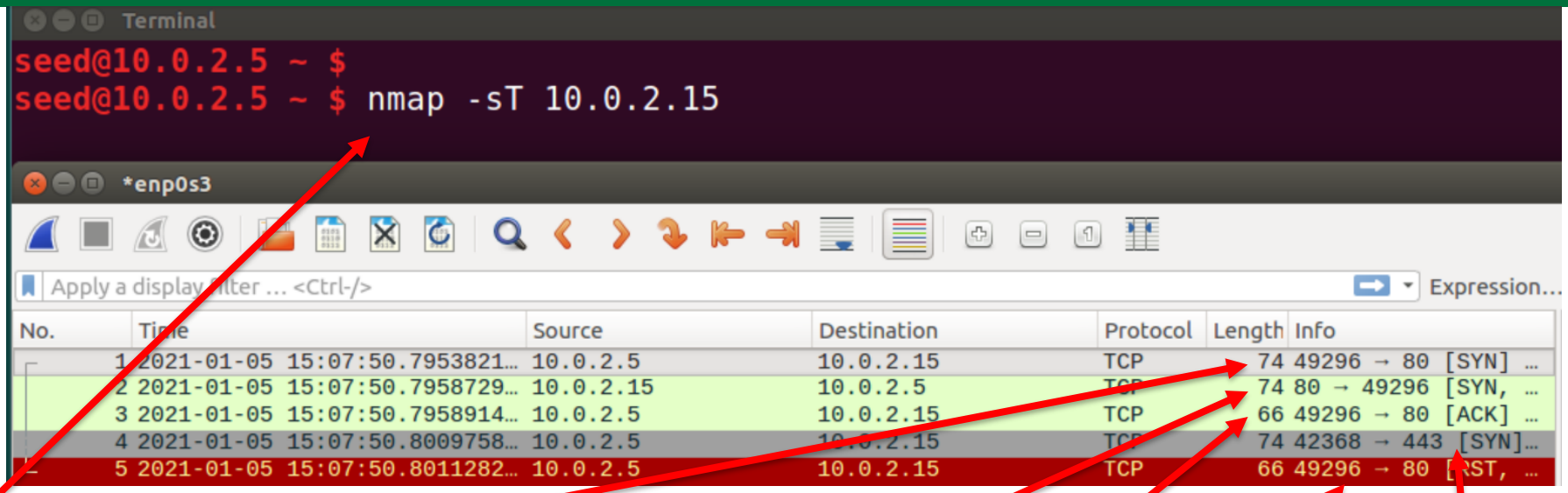
```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-05-05 14:48 EST
Nmap scan report for 10.0.2.15
Host is up (0.00098s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http
```

TCP uses a 3-way handshake



Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

Step 2: check for open ports



Run scan

Syn from 10.0.2.5 to target 10.0.2.15 on port 80

Syn/Ack from 10.0.2.15 to 10.0.2.5

Ack from 10.0.2.5 to 10.0.2.15

10.0.2.5 closes connection on port 80 with reset command

Next port, 443 already started

Discussion: make our own Intrusion Detection System (IDS)

Is scanning hosts and ports a “normal” activity?

No, it suggests a potential network intruder

How could we detect these intruders (Intrusion Detection System = IDS)?

Pseudo code a detector to see if a host is being port scanned

- Probably want some kind of time window (e.g., forget scans from long ago)
- Probably want some kind of threshold (e.g., 1 request may not be enough to cause alarm)
- Create hash table with entries: src -> List((time, port), (time, port))
- Sound alarm if more than threshold scans within time window

Example code posted on course web site for today

Step 3: scan around the IDS

use stealth mode to do half-open scan

$ sudo nmap -sS -D 10.0.2.6 –T2 10.0.2.15

Do NOT anger the IDS!

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-05-05 15:21 EST
Nmap scan report for 10.0.2.15
Host is up (0.00022s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http
MAC Address: 08:00:27:F2:D2:08 (Oracle VirtualBox virtual NIC)
```

-sS flag means do a half-open scan
Sends SYN, but followed by RST to close
Might draw less attention from the IDS

-D flag sends a decoy packet spoofed to come from another IP address (10.0.2.6) making it difficult to tell who is the real attacker!

-T2 scans slowly (T0 to T4; T3 is normal speed, T4 is parallel fast scan)

Defender wants P > D + R
Adversary wants to avoid D, so slow down scan to avoid trigger IDS

Step 4: perform banner grabbing, use O flag to get OS versions

use –O flag to get OS version

$ sudo nmap -O 10.0.2.15

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-05-05 15:24 EST
Nmap scan report for 10.0.2.15
Host is up (0.00057s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http
MAC Address: 08:00:27:F2:D2:08 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
```

First ping host to ensure up

Use TCP 3-way handshake to see what ports are up

This scan will probably anger the IDS!

Returns MAC address

Correctly detects this is a Linux machine

Step 4: perform banner grabbing, use A flag to get OS version and service versions

use –A flag to get OS version and service versions!

$ sudo nmap -A 10.0.2.15

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-05-05 15:29 EST
<snip>
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        vsftpd 3.0.3
22/tcp  open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4b:6f:e9:4a:8e:5b:2b:4d:12:34:94:48:9b:fc:05:1a (RSA)
|_  256 37:61:b8:e9:07:af:1c:f1:6a:49:94:ea:de:19:cf:b4 (ECDSA)
23/tcp  open  telnet     Linux telnetd
53/tcp  open  domain     ISC BIND 9.10.3-P4-Ubuntu
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp  open  http       Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
<snip>
TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 10.0.2.15
<snip>
```

FTP and SSH versions based on banners

SSH key!

Telnet, DNS, and web server versions based on banners

This scan will probably anger the IDS!

Also traceroute for good measure

Step 5: scan for vulnerabilities, use script vuln to run vulnerability scans

use –script to run script, vuln runs vulnerability scans !

$ sudo nmap –script vuln 10.0.2.15

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-05-05 15:46 EST
Nmap scan report for 10.0.2.15
Host is up (0.00035s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
53/tcp  open  domain
80/tcp  open  http
|_http-cross-domain-policy: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| <snip>
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
```

Scan takes a while

Took 6.5 minutes to scan one host in my VM

We have barely scratched the surface on what nmap can do

Vulnerable to slow loris attack (https://www.youtube.com/watch?v=XiFkyR35v2Y)

This scan will probably also anger the IDS!

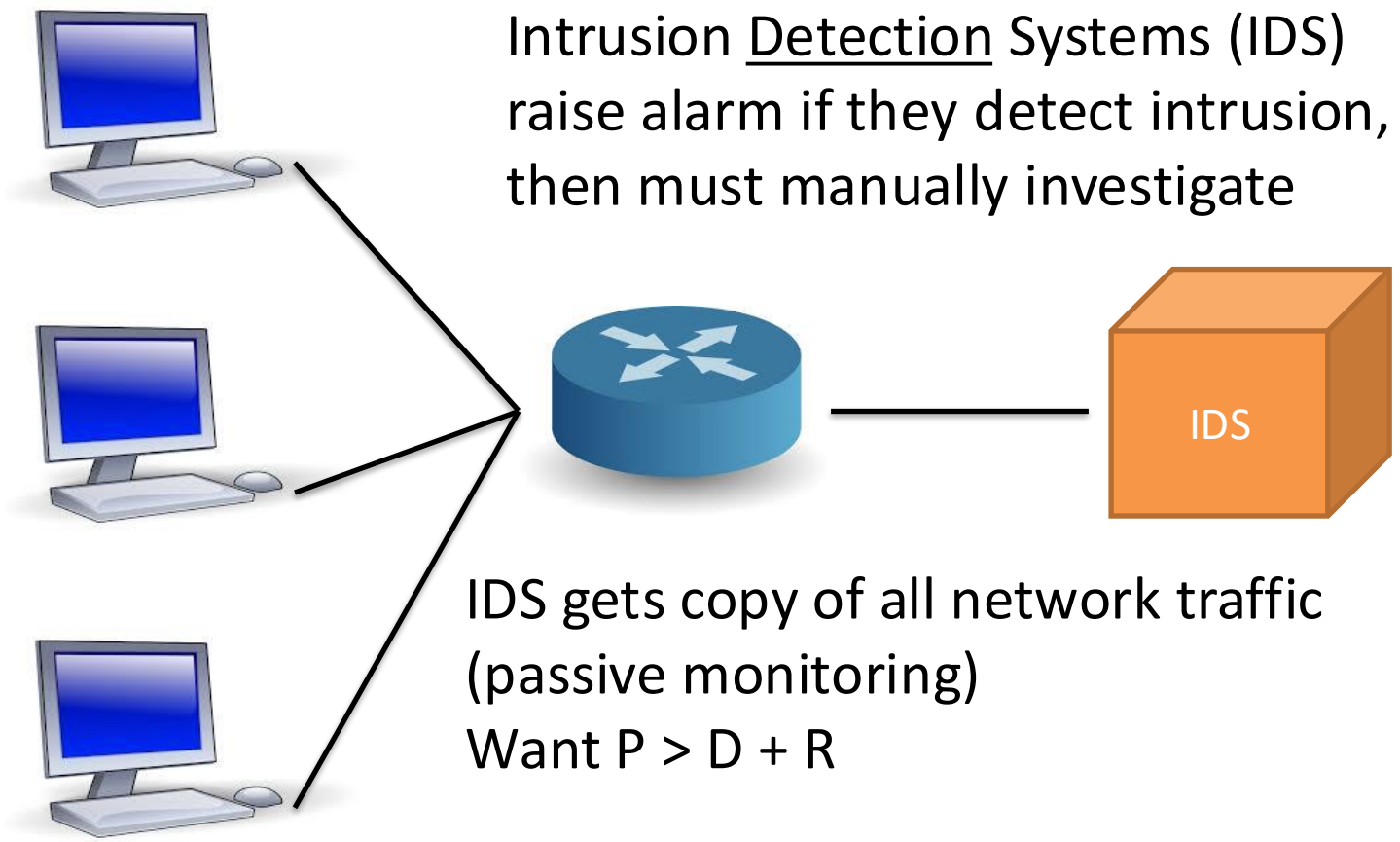
Agenda

1. Penetration testing
2. Network scanning
3. IDS/IPS
4. Incident response planning
5. Economics
6. Certifications

IDS watch traffic to identify adversaries

Intrusion Detection System

- Look for exploits against systems, applications, etc.
- Buffer overflows, XSS, SQL injections, other vulnerabilities

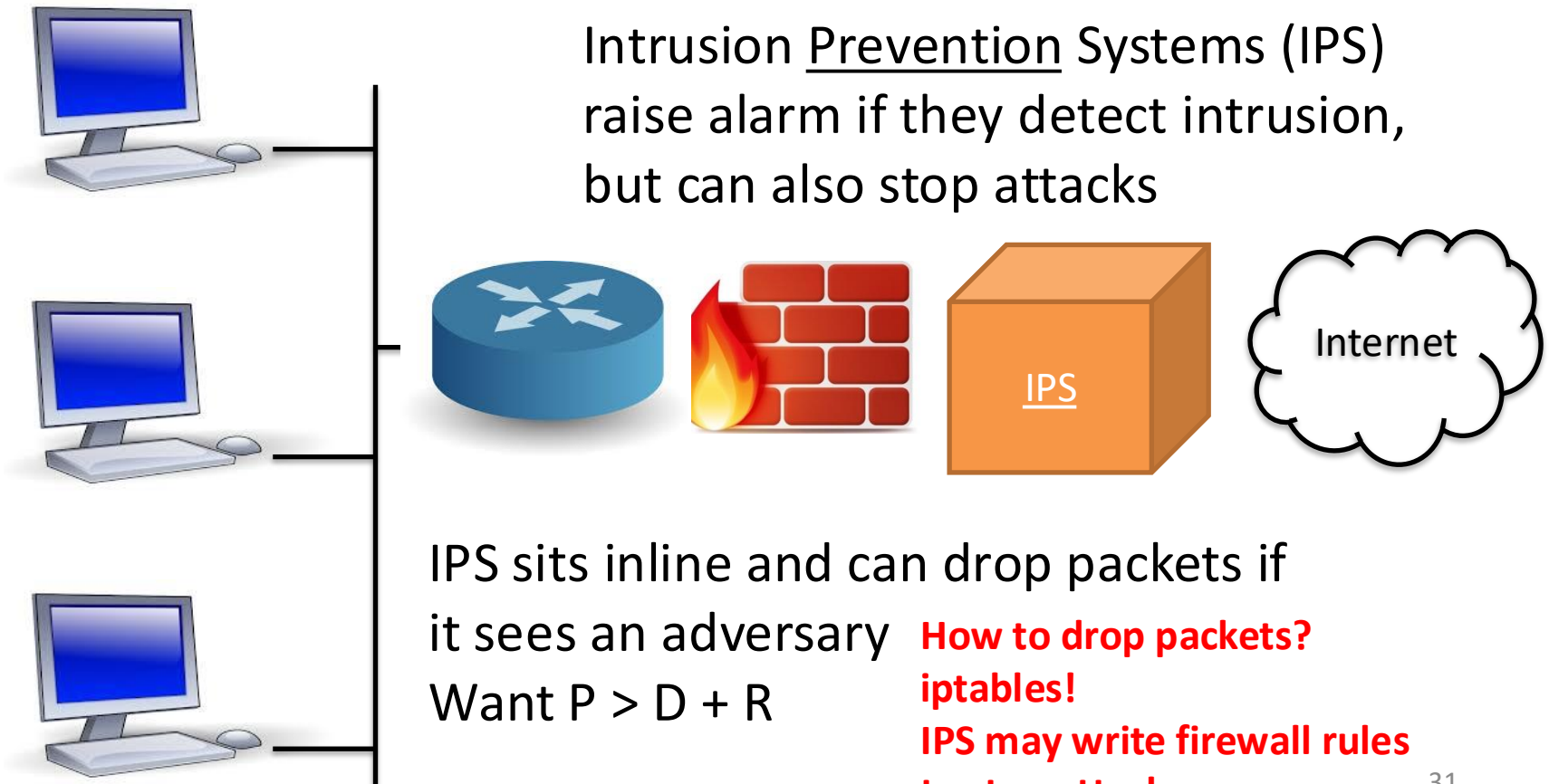


Adapted from https://www.professormesser.com/security-plus/sy0-501/network-intrusion-detection-and-prevention-3/

IPS watch traffic to identify adversaries and may take action to stop them

Intrusion Prevention System

- Look for exploits against systems, applications, etc.
- Buffer overflows, XSS, SQL injections, other vulnerabilities



Intrusion Prevention Systems (IPS) raise alarm if they detect intrusion, but can also stop attacks

IPS sits inline and can drop packets if it sees an adversary

Want P > D + R

How to drop packets?
iptables!
IPS may write firewall rules to stop attack

Adapted from https://www.professormesser.com/security-plus/sy0-501/network-intrusion-detection-and-prevention-3/

There are several ways to detect an adversary, none are perfect

Signature/rule-based

- Look for perfect match with known intrusion signatures
- Very common approach
- Must update signatures like anti-virus

IDS/IPS actions based on a set of rules you define

- **Block malware**
- **May allow some actions but still alert or log event**

Anomaly-based

- Build baseline on what is normal
- When a device does something unusual, the IDS/IPS alerts or prevents

Hard to balance false alarms vs false negatives

Behavior-based

- If file deleted or other changes made, block action or raise alarm

Heuristics

False negatives can be worse than false positives, but alarm fatigue can occur with false positives!

Can be time consuming to research and resolve

- Use artificial intelligence to detect intrusion
- No signatures, set of characteristics of attack

Adapted from https://www.professormesser.com/security-plus/sy0-501/network-intrusion-detection-and-prevention-3/

Snort is a popular free and open-source IDS/IPS system

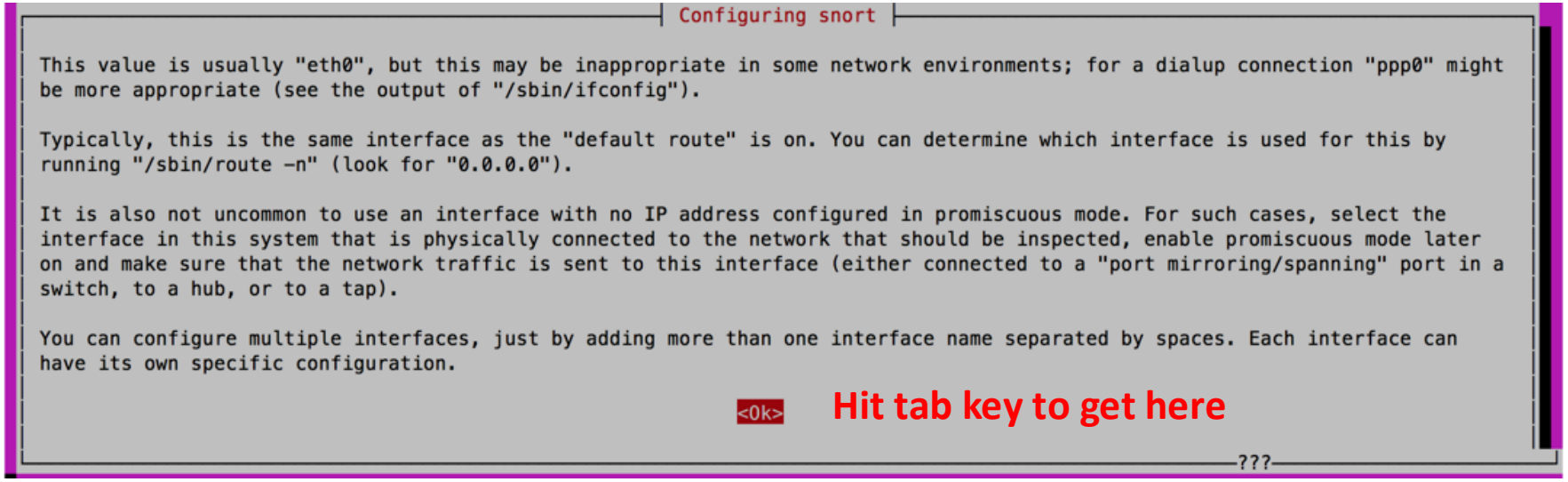


Snort

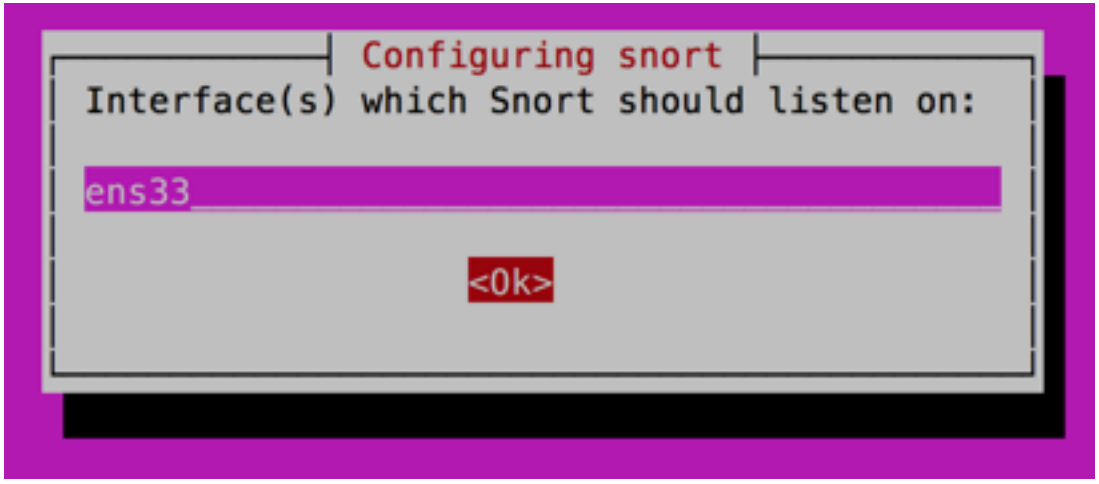
- Open source IDS/IPS
- Originally developed in 1998
- Now part of Cisco Talos
- Rule based
- Can write custom rules
- Can subscribe to Cisco rules

You can install Snort on your VM

$ sudo apt install snort –y

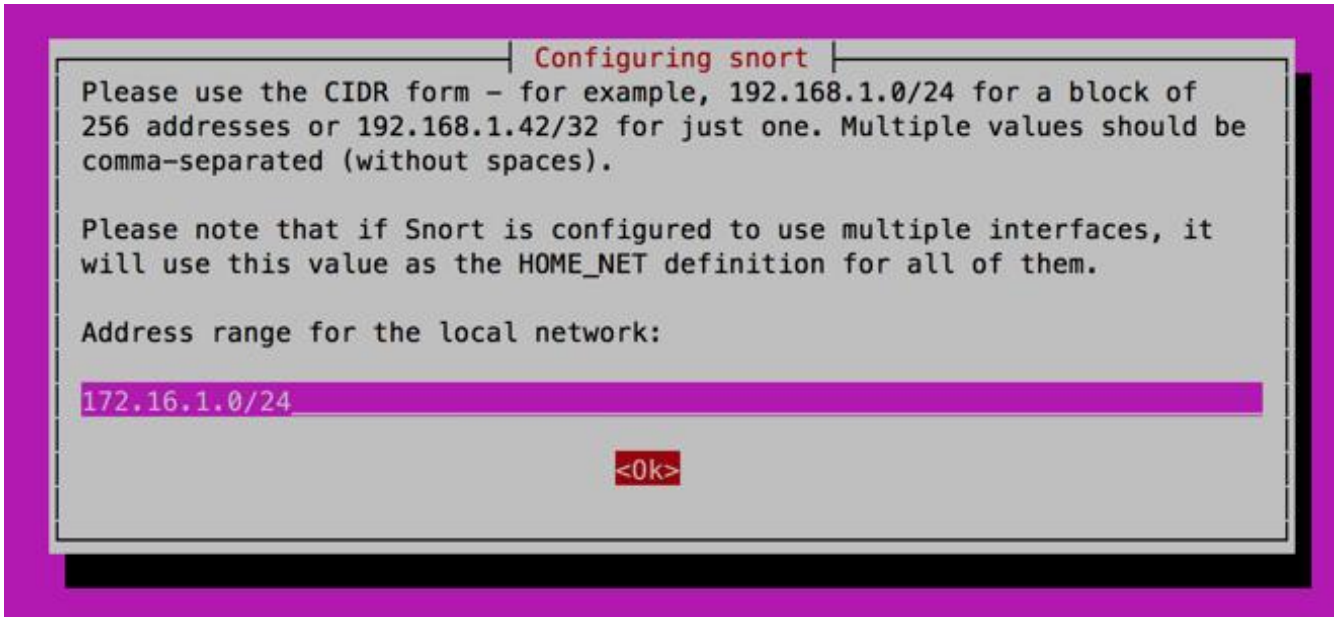


Hit tab key to get here



Use ifconfig to find your interface

You can install Snort on your VM



Run with

$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

-A: send alerts to console
-q: quiet mode (suppress start up banner and status report)
-u snort –g snort: run in group snort with user snort
-c: rules file, can edit to tell what snort should look for, then look for it
-i: interface

Suricata seems to be replacing Snort as the free IPS of choice for many organizations

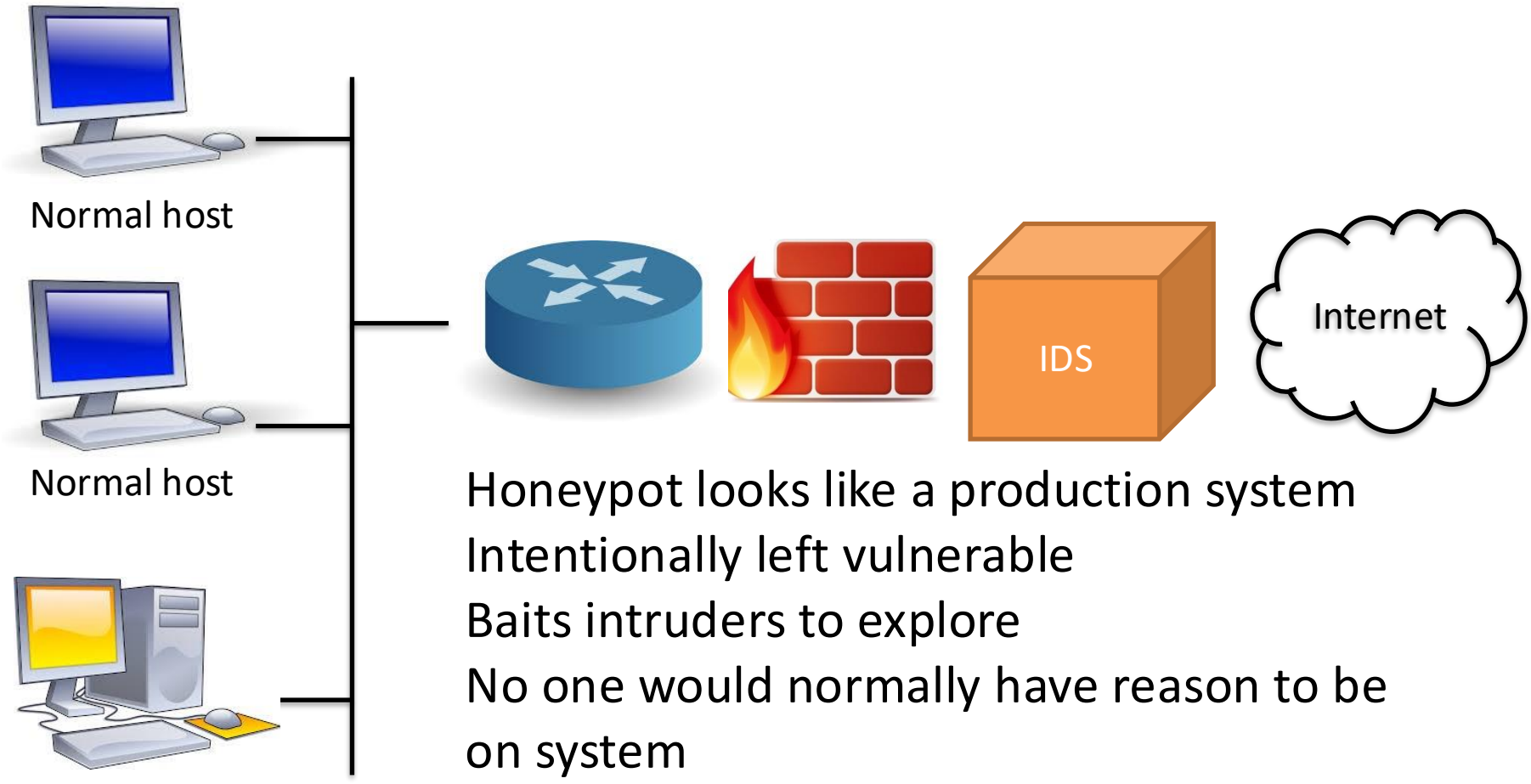




Feature	Snort	Suricata
Architecture	Traditionally single-threaded (though Snort 3 introduced multi-threading)	Natively multi-threaded, offering better performance on high-speed networks
Rule compatibility	Standard Snort rules	Compatibility with Snort rules; has its own set of rules
Logging	Basic logging	Network Security Monitoring in JSON format, easier integration with SIEM
Popularity	Widely deployed, industry standard	Growing in popularity

Adapted from: https://www.stamus-networks.com/suricata-vs-snort

Honeypots are designed to attract intruders and can be like an IDS



Honeypot looks like a production system
Intentionally left vulnerable
Baits intruders to explore
No one would normally have reason to be on system
Access alerts staff to intruder's presence
Acts like lightweight IDS
Many honeypots together called honeynet

Discussion

IDS detects someone on the network running John the Ripper (password guessing program) to gain root access on server

What do you do?

Agenda

1. Penetration testing
2. Network scanning
3. IDS/IPS
4. Incident response planning
5. Economics
6. Certifications

An incident response plan is a set of instructions to respond to security events

Goal: allow an organization to respond efficiently to a security-related event

Steps to create an incident response plan

- Identify an incident recovery team
- Determine critical components of the network
- Identify single points of failure and address them
- Create a disaster recovery plan
- Create an incident response plan
  - List roles and responsibilities
  - Summarize tools, technologies, and physical resources that must in place
  - List critical network and data recovery processes
  - Plan for communications, both internal and external
- Train staff/practice plan

Disaster recovery plan usually aimed at physical disasters
Plan from local (pipe breaks) to regional (hurricane) issues

Incident response plan aimed at security events

Important and ongoing!
Systems must work, but people need to know what to do
One group works from back up facility once/month

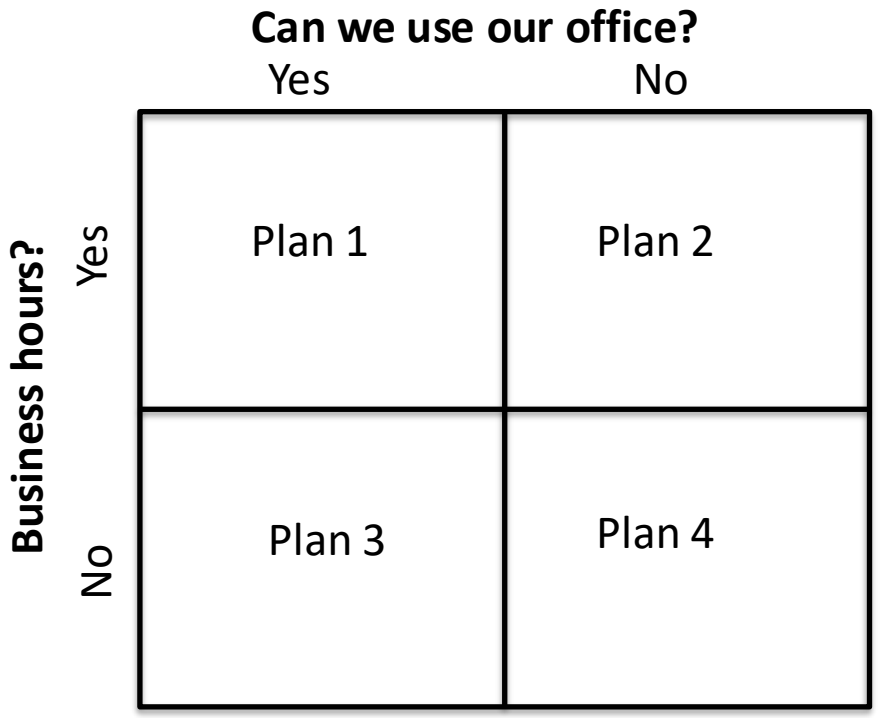
Adapted from https://www.cisco.com/c/en/us/products/security/incident-response-plan.html#~how-to-create-a-plan

Make a *useable* plan

Once hired a firm to help us develop a disaster recovery plan
They wanted to write huge tome of every scenario we might face
Problem:

Whatever happens probably won't match a scenario in the plan

My idea:



Each plan:

- How will we communicate with our employees?
- What order will be bring up systems?
  - Who will do what?
  - What credentials do we need?
- How will employees get their job done?

Agenda

1. Penetration testing
2. Network scanning
3. IDS/IPS
4. Incident response planning
5. Economics
6. Certifications

Discussion



Every dollar that you spend on security comes out of my bonus!

Why are you spending so much on security?!?!?

What do you say?

If something happens, you'll find me in Montana, or better yet, you won't find me in Montana!

Annualize Loss Expectancy (ALE) is a common way to justify security spending



You shouldn't spend $5,000 on a safe to protect a $2 item

How much should you spend?

ALE = damage * probability

Pierson's comments from the trenches:

- ALE is easy to say but hard to use in practice
- Some things are hard to value
  - Customer confidence in firm if event happens
  - Staff morale
- Estimating the probability of an adverse event is also difficult
- Be wary of vendor's estimation of threats – they have an agenda!

Adapted from Cole, Eric. *Advanced persistent threat: understanding the danger and how to protect your organization.* Syngress, 2013.

NY hedge fund ALE example: spending on disaster/incident preparedness

NY Hedge Fund post 9/11, after black out of Aug 14, 2003
ALE = annual loss expectancy = loss * probability

Fund size: 10B
Long term return: 15%
So, need to make $1.5B/year or with 252 trading days/year = $6M every day

What are the odds of something occurring that takes us down for 1 day during a year?

- If 10% likely, we should spend $6M * 0.10 = $600K/year
- We are spending less than $200K/year

What about the odds of something taking us down for 2 days?

You are getting a bargain!

You can think of spending on disaster/incident preparedness like paying for insurance

Another approach is to benchmark spending by other firms in the industry

Gartner

FORRESTER®

IDC
ANALYZE THE FUTURE

Industry overall spends >$120B on security hardware, software and services

Many firms survey industry participants and gather data about security spending

These firms sell reports summarizing their findings

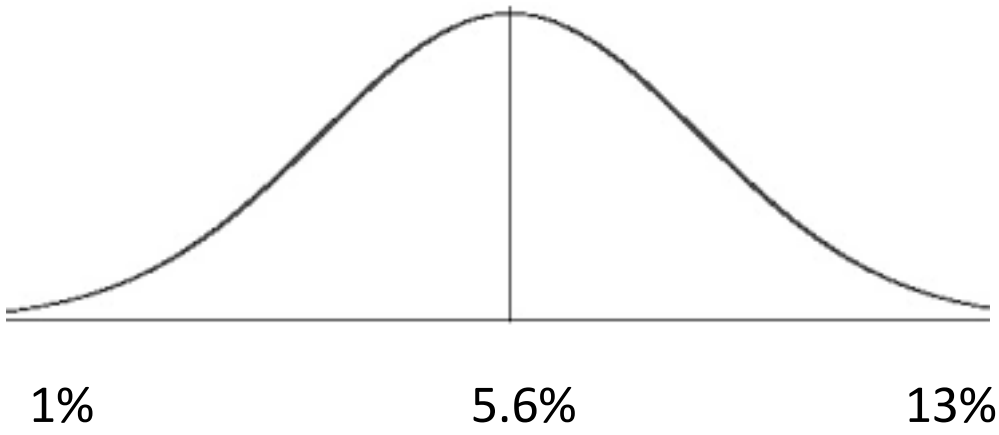
You can find how much your industry spends on security (and other items)

Normally presented as a percentage of sales

https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget

Companies tend to spend around 5% of their IT budget

Security spending as percentage of IT budget



Typically ranges from 1% to about 13% of IT budget

- Varies by industry
- Financial firms tend to spend more than firms in other industries

"We never had a cybersecurity budget until recently when I said we need a dedicated budget for it.

So, they took a chunk of the IT budget and told me to be grateful!

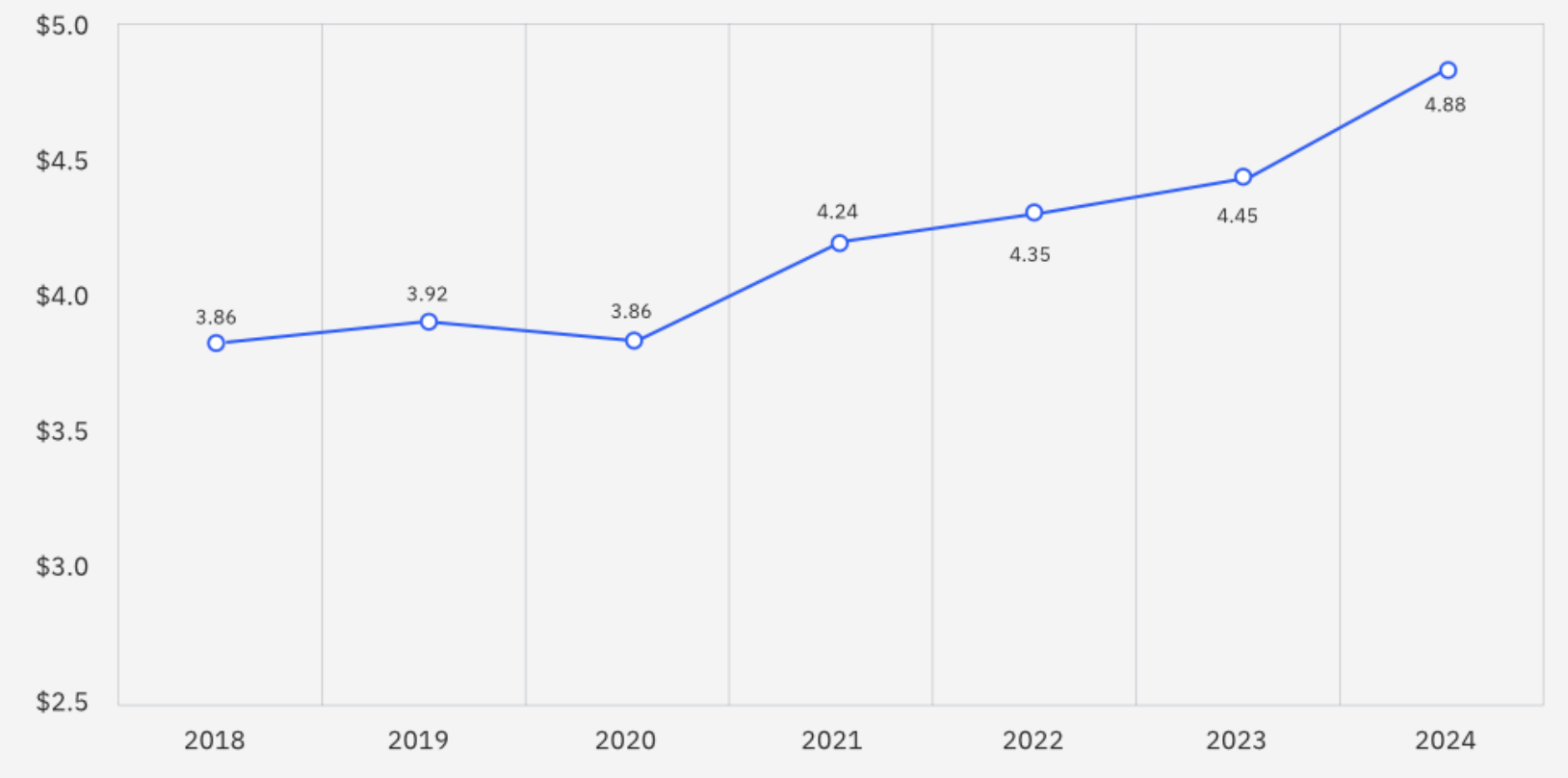
We have no more money overall, but some for cybersecurity!"
- Anonymous CISO

https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget

IBM found the global average cost of each data breach in 2024 was $4.88M

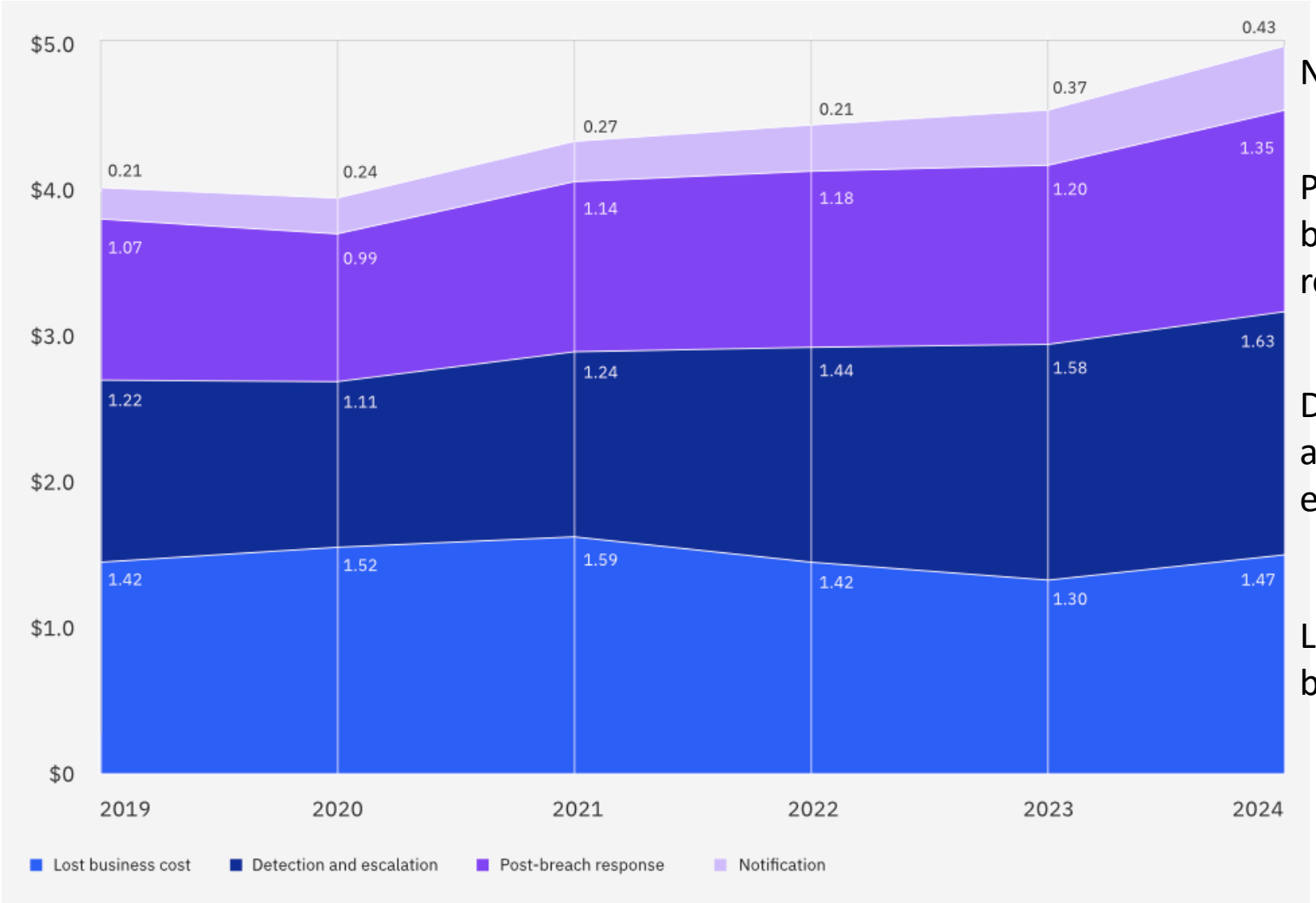
Global average cost ($M)

Average cost of a breach has been steadily rising



https://www.ibm.com/reports/data-breach

Costs are not limited to detection and escalation of the incident



Notification

Post-breach response

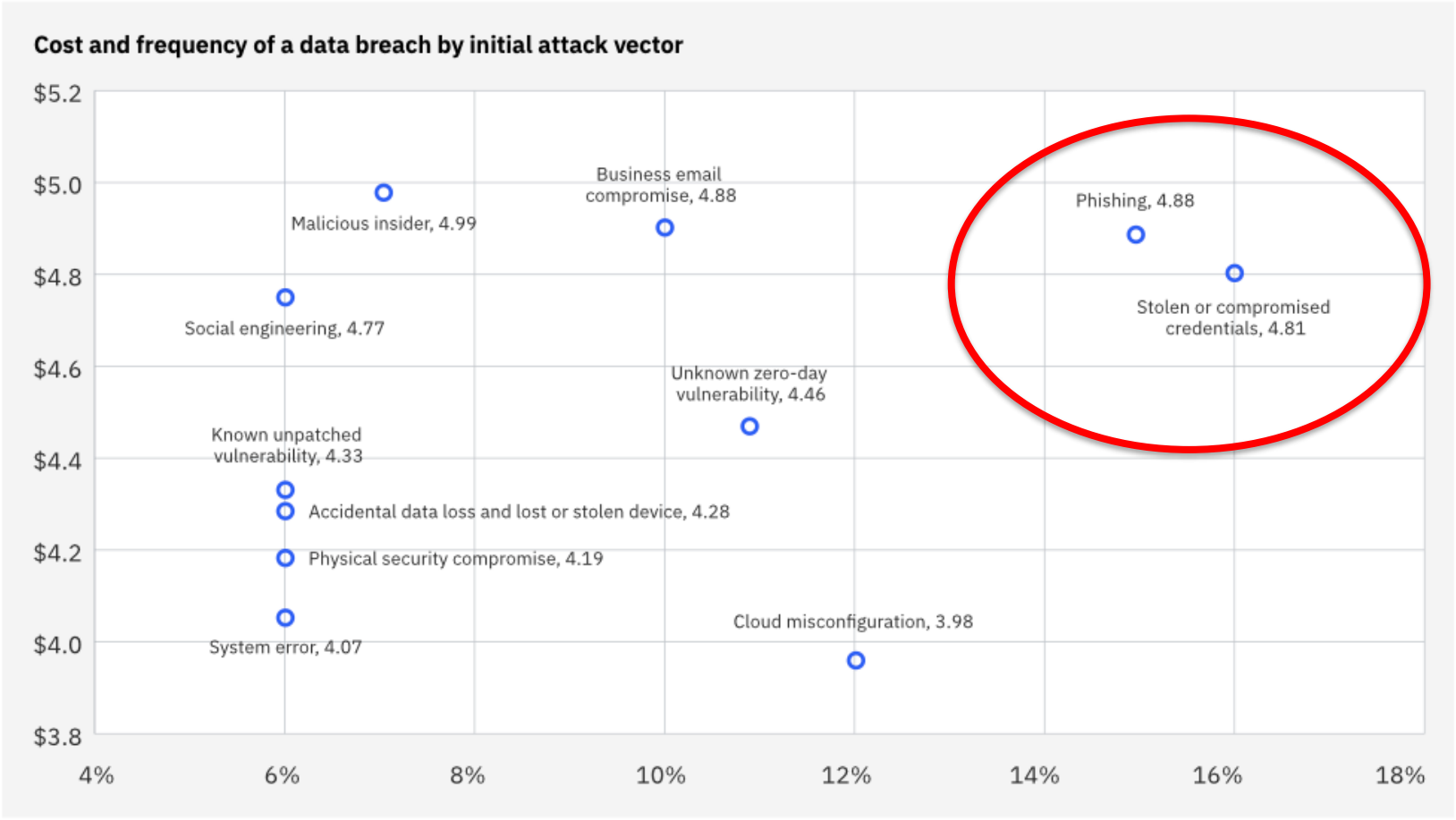
Detection and escalation

Lost business

https://www.ibm.com/reports/data-breach

Phishing and lost/compromised credentials were the most common and costly causes

Root cause by threat vector



https://www.ibm.com/reports/data-breach

Pierson's method of prioritizing projects

Every department in an organization has projects they consider vitally important

There are normally more projects in an organization that a technology department can simultaneously work on at any given time

Result: some projects wait, project owners grumble and fume



Department heads whose projects are not being addressed get angry… at you!

May turn to "Shadow IT"
Security implications? Now with AI?

Security must fight for prioritization

Pierson's method of prioritizing projects

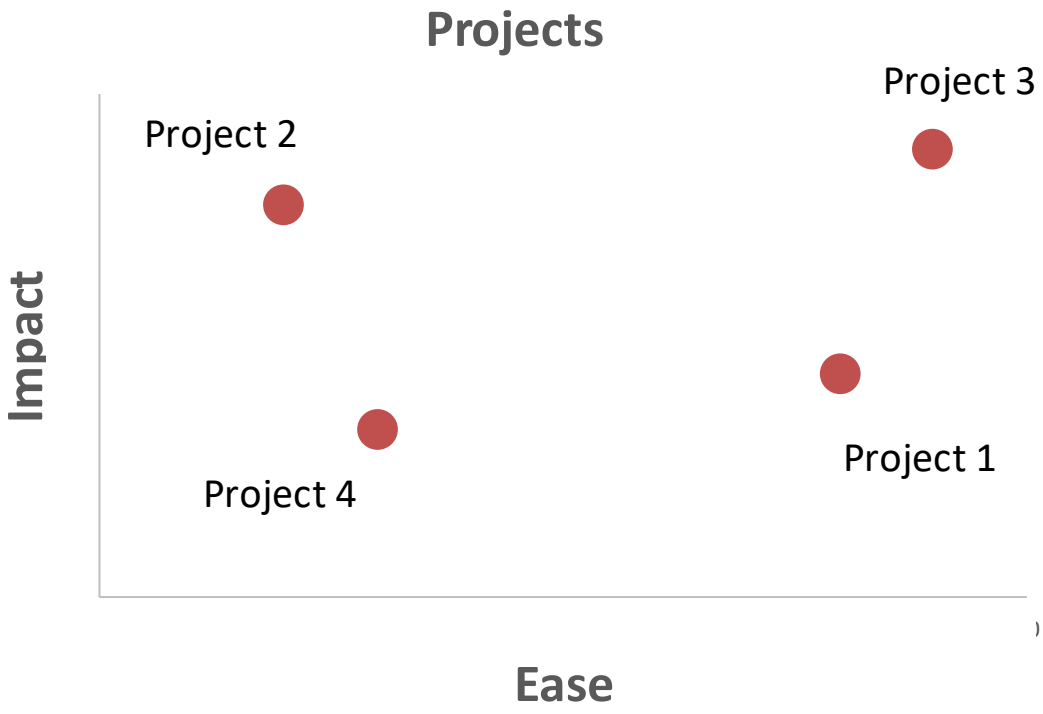
Quarterly meeting with all department heads

Each brings their most important projects

I rate each project on ease

The *group* rates each project on business impact

Plot projects on XY scatter graph



Note: business leaders decide *together* the importance to the overall *organization* of each project (including security)

Urgency baked into impact (but could plot as size of circle)

Pro tip: do not put numbers on axis while discussing

Pierson's method of prioritizing projects

Quarterly meeting with all department heads

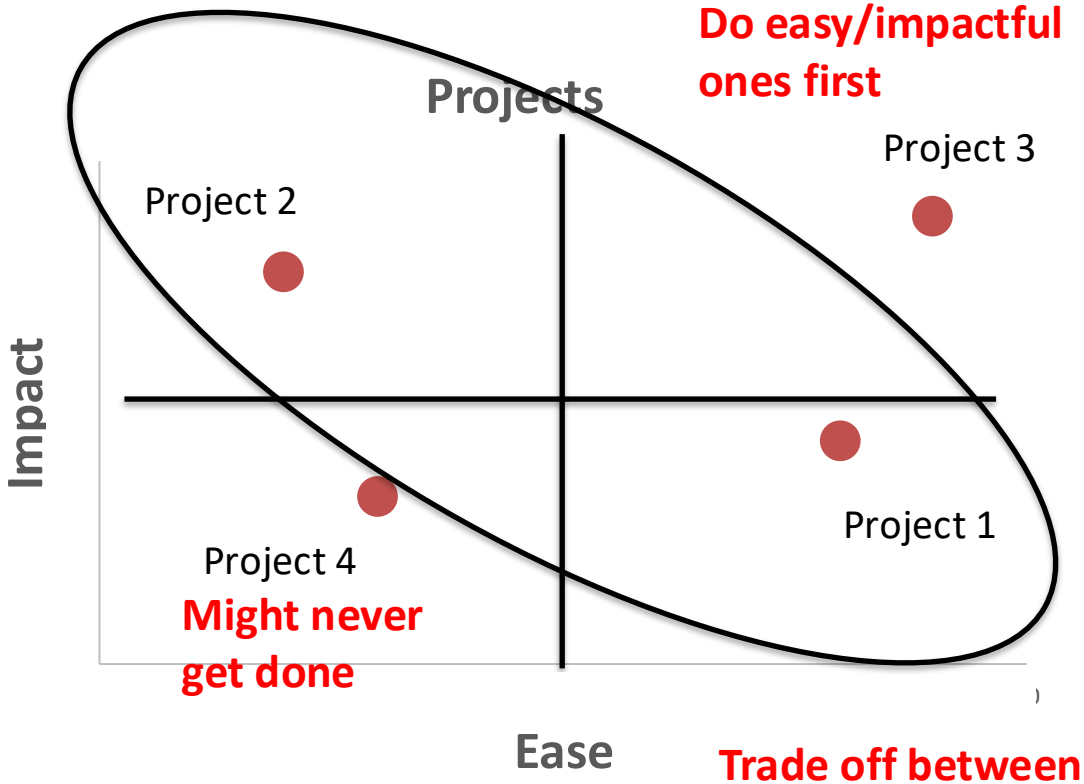
Each brings their most important projects

I rate each project on ease

The *group* rates each project on business impact

Plot projects on XY scatter graph

Repeat next quarter to ensure priorities haven't changed



Do easy/impactful ones first

Might never get done

Break projects into quadrants

Trade off between easy/not impactful and hard/impactful

Now business leaders have a justification for how and why projects were prioritized

Order based on resources needed

Agenda

1. Penetration testing
2. Network scanning
3. IDS/IPS
4. Incident response planning
5. Economics
6. Certifications

Some resources if you are interested in becoming a pen tester

Certified Ethical Hacker (CEH)

- Developed by the EC-Council https://www.eccouncil.org
- Oldest testing certification

GIAC Penetration Tester (GPEN)

- Developed by SANS Institute https://www.giac.org/certification/penetration-tester-gpen
- SANS well known for security papers and training
- Expensive!
- I've heard it is difficult to self-study

Offensive Security Certified Professional (OSCP)

- Developed by Offensive Security https://www.offensive-security.com/pwk-oscp/
- Not a written test, must successfully hack into test system

Certified Information System Security Professional (CISSP)

- Requires four years of experience with college degree (or five years without degree)
- "Any IT professional will need to get the CISSP at some point"

Easttom II, William Chuck. *Penetration testing fundamentals: A hands-on guide to reliable security audits*. Pearson IT Certification, 2018.

Some resources if you are interested in becoming a pen tester

Red Team Alliance

- Physical penetration testing
- Conduct training at their lab
- https://www.redteamalliance.com/



Physical Access Control Systems: Practical Hacking and Defense of RFID PACS

$2,650.00

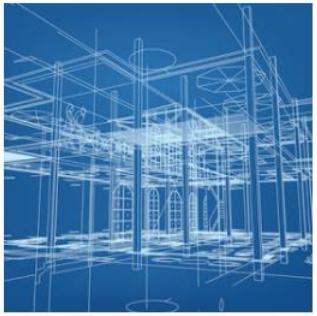
View Details and Dates



Covert Methods of Entry: 5-Day Intenstive

$3,750.00

View Details and Dates



Security Design Concepts: Designing Defensive Physical Security

$2,450.00

View Details and Dates



Surveillance Dynamics: Practical Tools, Tactics, and Techniques

$2,450.00

View Details and Dates



Physical Intrusion Detection Systems: Practical Hacking and