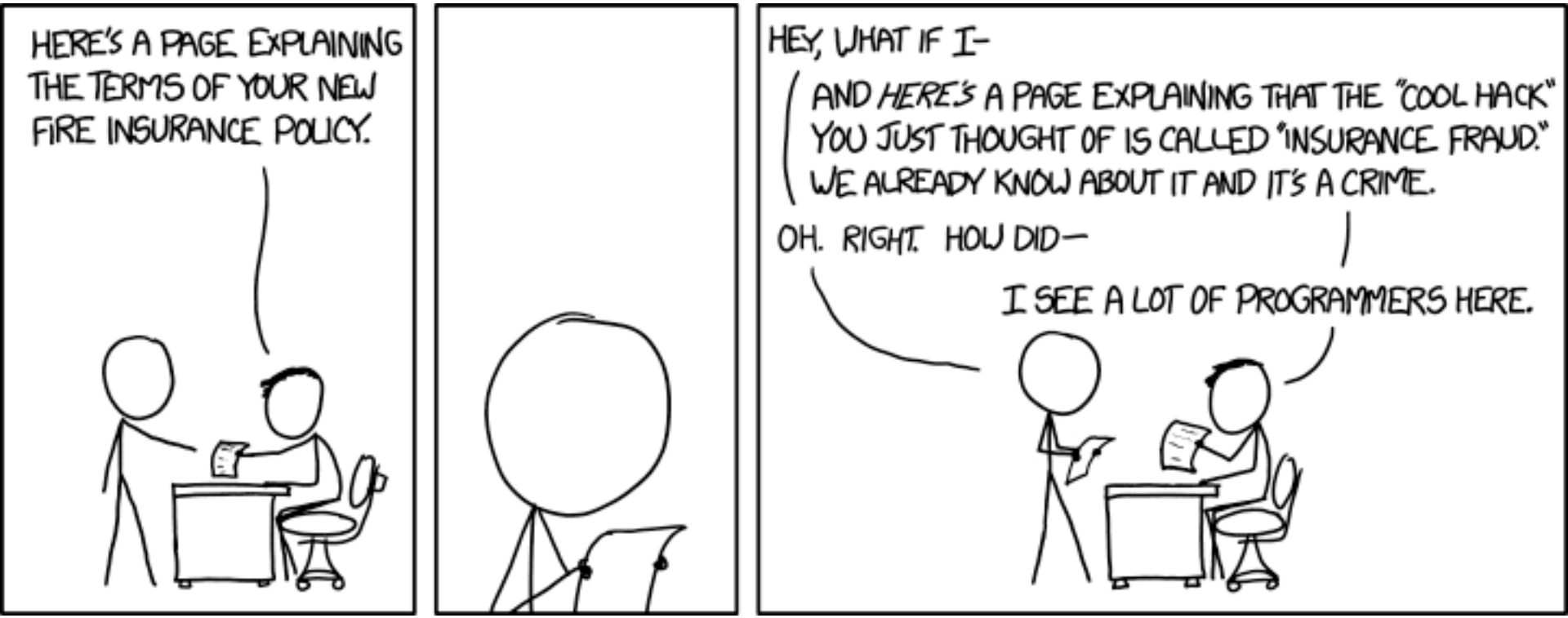
CS 55:
Security and Privacy

Pen testing; IDS/IPS; network scanning



https://xkcd.com/1494/

Agenda

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

Discussion

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

Penetration testing: find/fix vulnerabilities before adversaries exploit them

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

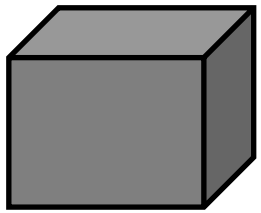
- Try to exploit people, process, and technology
- Simulate an adversary trying to gain access
- Fix problems before exploited

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

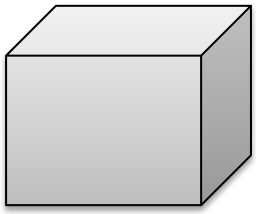
A penetration test simulates an attack on a system

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

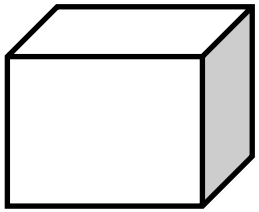
Penetration tests (aka ethical hacking, white hat hacking) try to gain access and escalate privileges



Black box
Testers given no knowledge of network



Grey box
Testers given some knowledge of network



White 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?

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

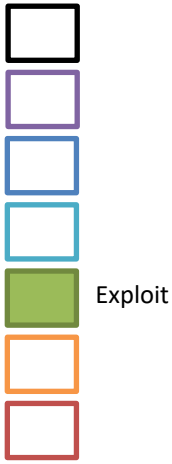
Pre-engagement interactions	• Define scope/expectations • Create clear contract
Intelligence gathering	• OSINT • Other intel (may be client provided)
Threat modelling	• Contemplate threats (APT, script kiddies) • Model their likely approach
Vulnerability analysis	• Run vulnerability scanners to find targets to exploit • Metasploit, Nmap, Vega, Nessus, Zap
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
2. **Active scanning**
   - Scan ports on all available IP addresses (nmap)
   - Run vulnerability scanners (nmap, Vega, Nessus, ZAP, Metasploit)
   - Risk of detection increased
3. **Breaching**
   - Manually conducting exploits (buffer overflows, SQL attacks, XSS)
   - Phishing
   - Metasploit/harmless viruses
4. **Completion**
   - Fix holes

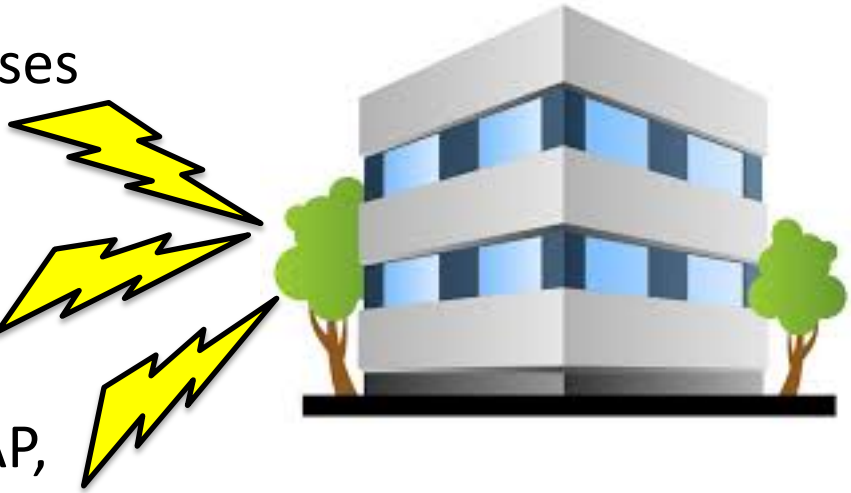


Adapted from Easttom II, William Chuck. *Penetration testing fundamentals: A hands-on guide to reliable security audits*. Pearson IT Certification, 2018.

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

1) External: test from outside

- Port scan all 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, Vega, 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

Discussion

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

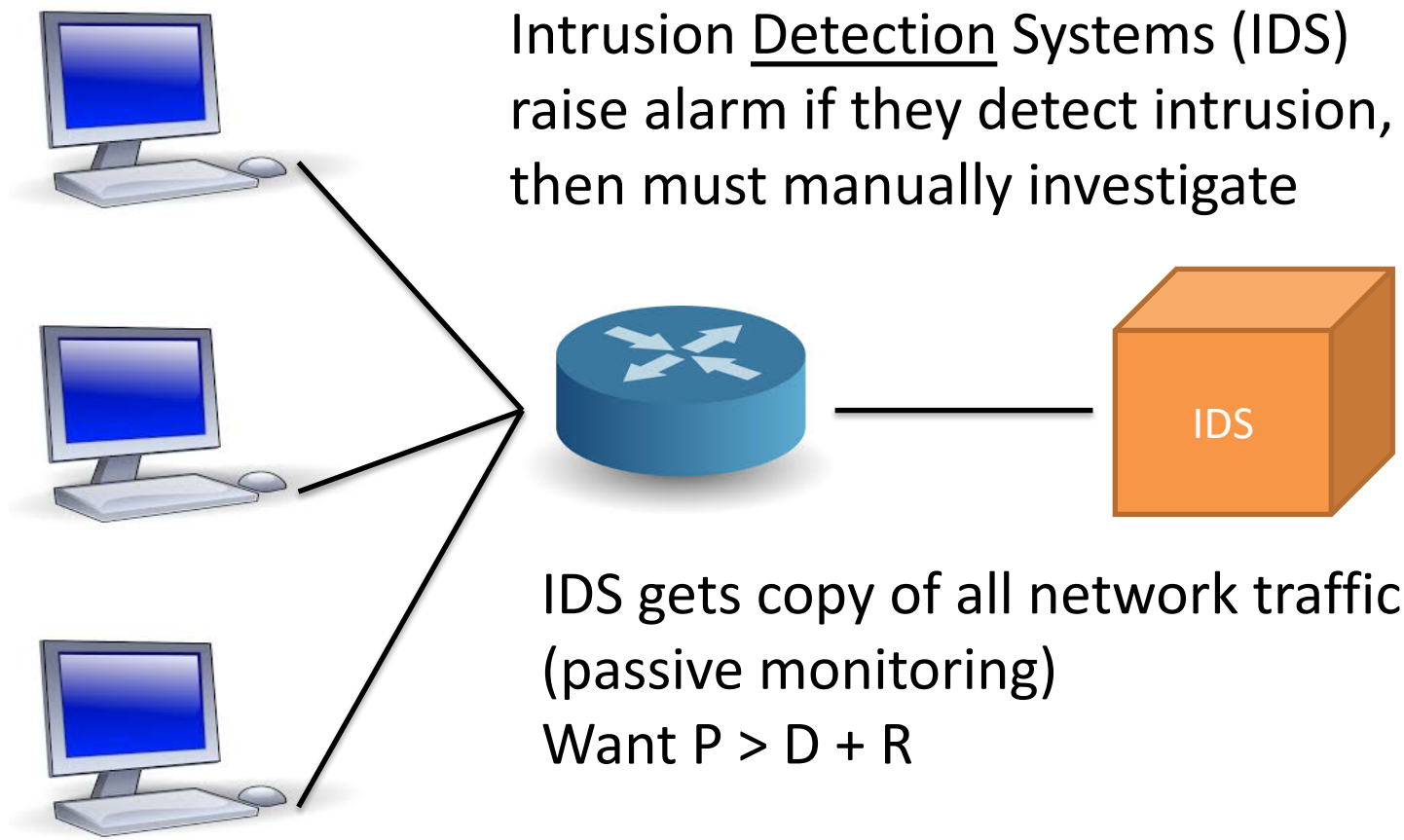
Agenda

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

IDS watch traffic to identify adversaries

Intrusion Detection System/Intrusion Prevention System

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



Intrusion Detection Systems (IDS) raise alarm if they detect intrusion, then must manually investigate

IDS gets copy of all network traffic (passive monitoring)

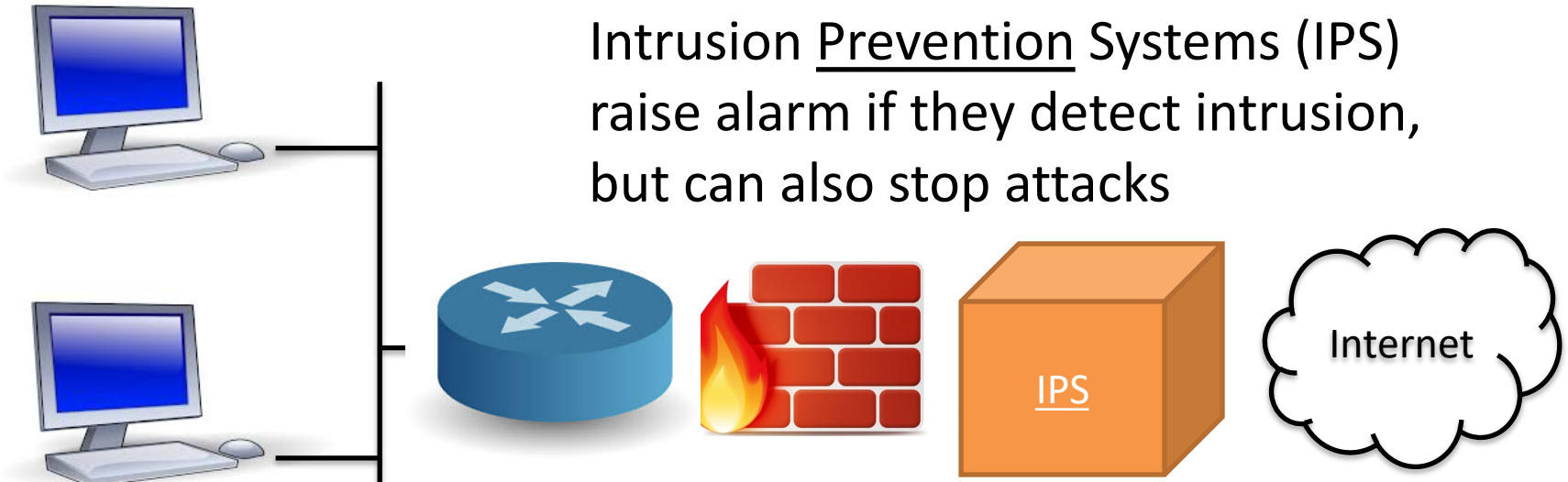
Want P > D + R

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 Detection System/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

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**
- **Allow some actions but alert**

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

Time-consuming to research and resolve

Heuristics

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

False negatives can be worse than false positives!

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

Snort is a popular IPS system

Snort

- Open source 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

```
Configuring snort

This value is usually "eth0", but this may be inappropriate in some network environments; for a dialup connection "ppp0" might
be more appropriate (see the output of "/sbin/ifconfig").

Typically, this is the same interface as the "default route" is on. You can determine which interface is used for this by
running "/sbin/route -n" (look for "0.0.0.0").

It is also not uncommon to use an interface with no IP address configured in promiscuous mode. For such cases, select the
interface in this system that is physically connected to the network that should be inspected, enable promiscuous mode later
on and make sure that the network traffic is sent to this interface (either connected to a "port mirroring/spanning" port in a
switch, to a hub, or to a tap).

You can configure multiple interfaces, just by adding more than one interface name separated by spaces. Each interface can
have its own specific configuration.

<Ok>
```

Hit tab key to get here

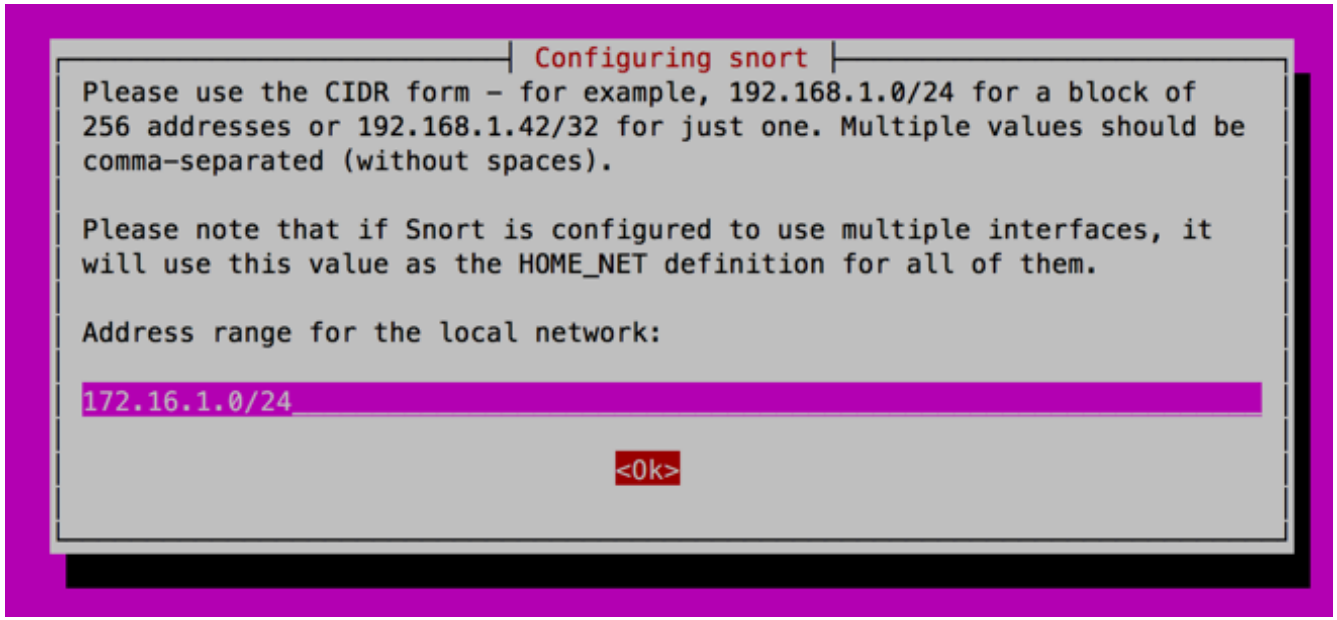
```
Configuring snort
Interface(s) which Snort should listen on:

ens33

<Ok>
```

Use enp0s3 (find with ifconfig)

You can install Snort on your VM



10.0.2.0/24

Run with

$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3

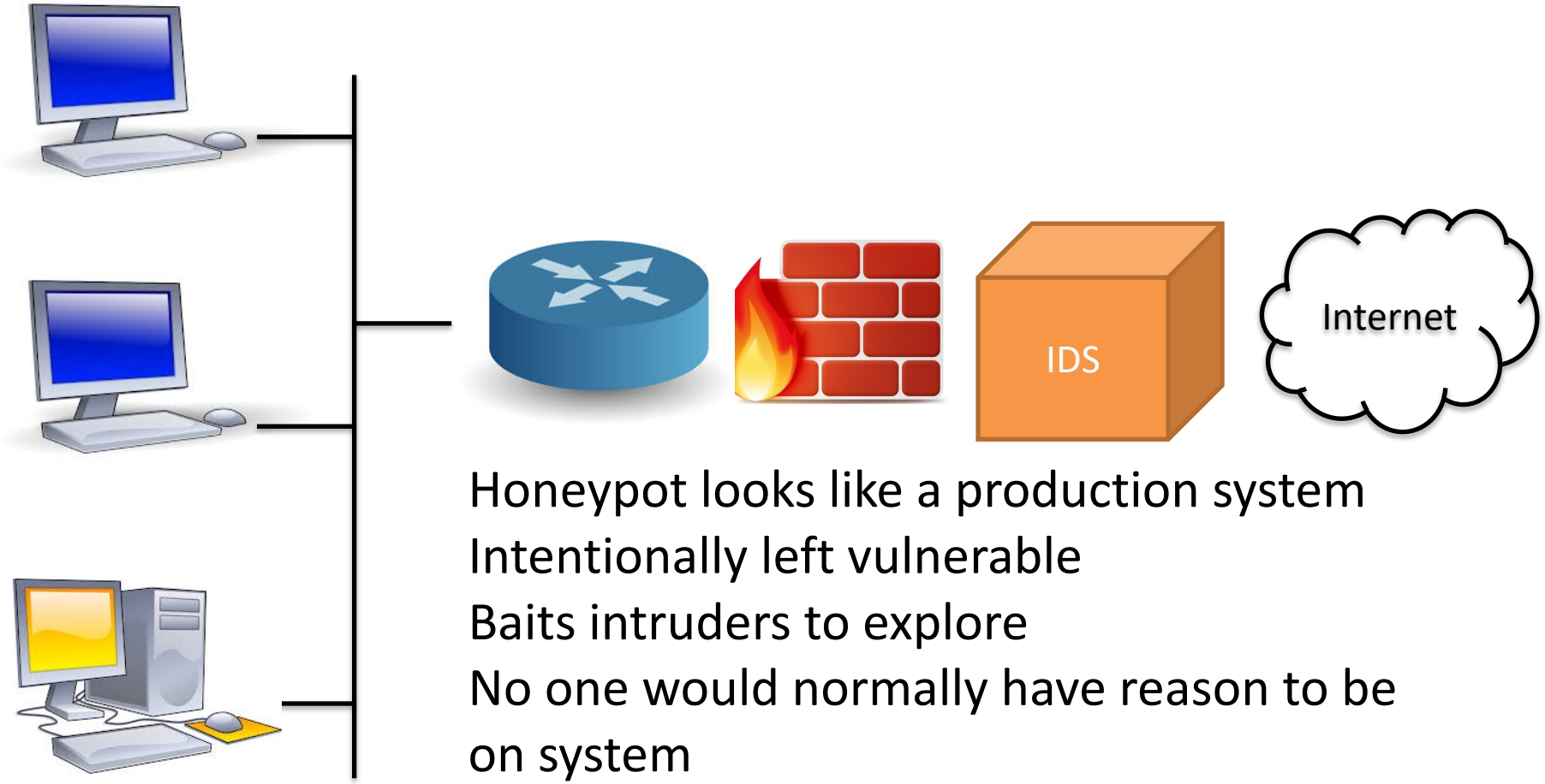
Snort demo

```
//see snort config on 10.2.15
$ sudo gedit /etc/snort/snort.conf
//Scroll down to step 7 and see snort rules
close gedit

//show mysql rules
$ cat /etc/snort/rules/mysql.rules

//start snort and show it running
$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3
From 10.0.2.5: $ ping 10.0.2.15
```

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



Honeypot

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

What do you do?

Agenda

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

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

www.netcraft.com

NETCRAFT

Site report for https://dartmouth.edu

Look up another site?

Share:

Background

Site title	Dartmouth College | Home	**Date first seen**	August 1995
Site rank	1328493	**Netcraft Risk Rating**	0/10
Description	One of the world's greatest academic institutions and a member of the Ivy League, Dartmouth has been educating leaders since 1769. Our undergraduate and graduate programs are distinguished by academic excellence, personal attention from top faculty, opportunities to participate in research, and a close-knit community.	**Primary language**	English

Network

Site	https://dartmouth.edu	**Domain**	dartmouth.edu

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

www.builtwith.com

Log In · Signup for Free

builtwith Tools Features Plans Customers Resources Website, Tech, Keyw

Home / dartmouth.edu Technology Profile

DARTMOUTH.EDU

Technology Profile | Detailed Technology Profile | Meta Data Profile | Relationship Profile | Redirect Profil

Misleading Technology Profile Warning

DARTMOUTH.EDU is on our misleading profile site list. This means that various pages across dartmouth.edu and its subdomains make it difficult for us to accurately tell you what this site is built with.

Profile Details

Link to this page.
updated 28th Fe

Analytics and Tracking — View Global Trends

New Relic

New Relic Usage Statistics · Download List of All Websites using New Relic

New Relic is a dashboard used to keep an eye on application health and availability while monitoring real user experience.

Application Performance

WF
Unlimited d
normally
$99
Bu
Learn more

Widgets — View Global Trends

Konami Code

Shodan.io scans the Internet for vulnerable devices

www.shodan.io

Shodan Developers Monitor View All... Try out the new beta website! Help Center

SHODAN Explore Pricing Enterprise Access New to Shodan? Login or Register

The search engine for the Web

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

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!

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.

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!

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

Adversaries will try to learn as much as possible about the network

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.

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 2021-01-05 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

Interesting target?

Pings all devices

Not many devices up on the VM's network

But now we know which IP address are in use

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 2021-01-05 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

Step 2: check for open ports

nmap can find all open ports on a particular computer

$ nmap -sT 10.0.2.15

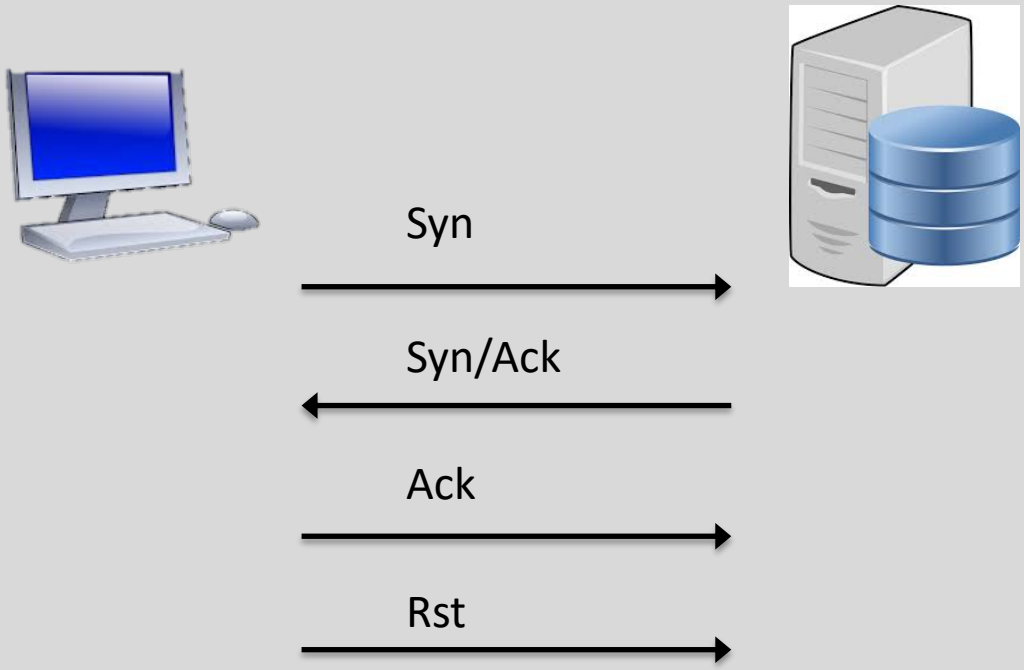
This command uses the whole 3-way handshake (full-open scan)
Noisy, iDS might detect, use –sS for syn scan (half-open scan)

Starting Nmap 7.01 (https://nmap.org) at 2021-01-05 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

TCP uses a 3-way handshake



Step 2: check for open ports

Terminal

```
seed@10.0.2.5 ~ $
seed@10.0.2.5 ~ $ nmap -sT 10.0.2.15
```

*enp0s3

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-01-05 15:07:50.7953821…	10.0.2.5	10.0.2.15	TCP	74	49296 → 80 [SYN] …
2	2021-01-05 15:07:50.7958729…	10.0.2.15	10.0.2.5	TCP	74	80 → 49296 [SYN, …
3	2021-01-05 15:07:50.7958914…	10.0.2.5	10.0.2.15	TCP	66	49296 → 80 [ACK] …
4	2021-01-05 15:07:50.8009758…	10.0.2.5	10.0.2.15	TCP	74	42368 → 443 [SYN]…
5	2021-01-05 15:07:50.8011282…	10.0.2.5	10.0.2.15	TCP	66	49296 → 80 [RST, …

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

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

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-05 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
Might draw less attention from the IDS

-D flag sends a duplicate 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)

Step 4: perform banner grabbing

use –O flag to get OS version

$ sudo nmap -O 10.0.2.15

```
Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-05 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

Correctly detects this is a Linux machine

Returns MAC address

Step 4: perform banner grabbing

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 2021-01-05 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

SSH key!

Telnet, DNS, and web server versions

This will attract the IDS's attention!

Also traceroute for good measure

Step 5: scan for vulnerabilities

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 2021-01-05 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
|       the http server's resources causing Denial Of Service
```

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

This scan will attract the IDS's attention!

Agenda

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

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

Agenda

1. Penetration testing
2. IDS/IPS
3. Network scanning
4. Incident response planning
5. 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!
- 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

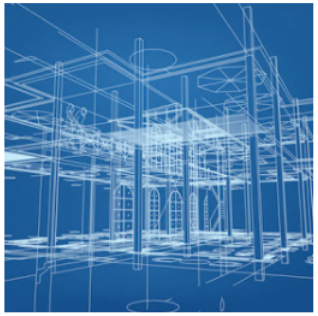
$2,650.00

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

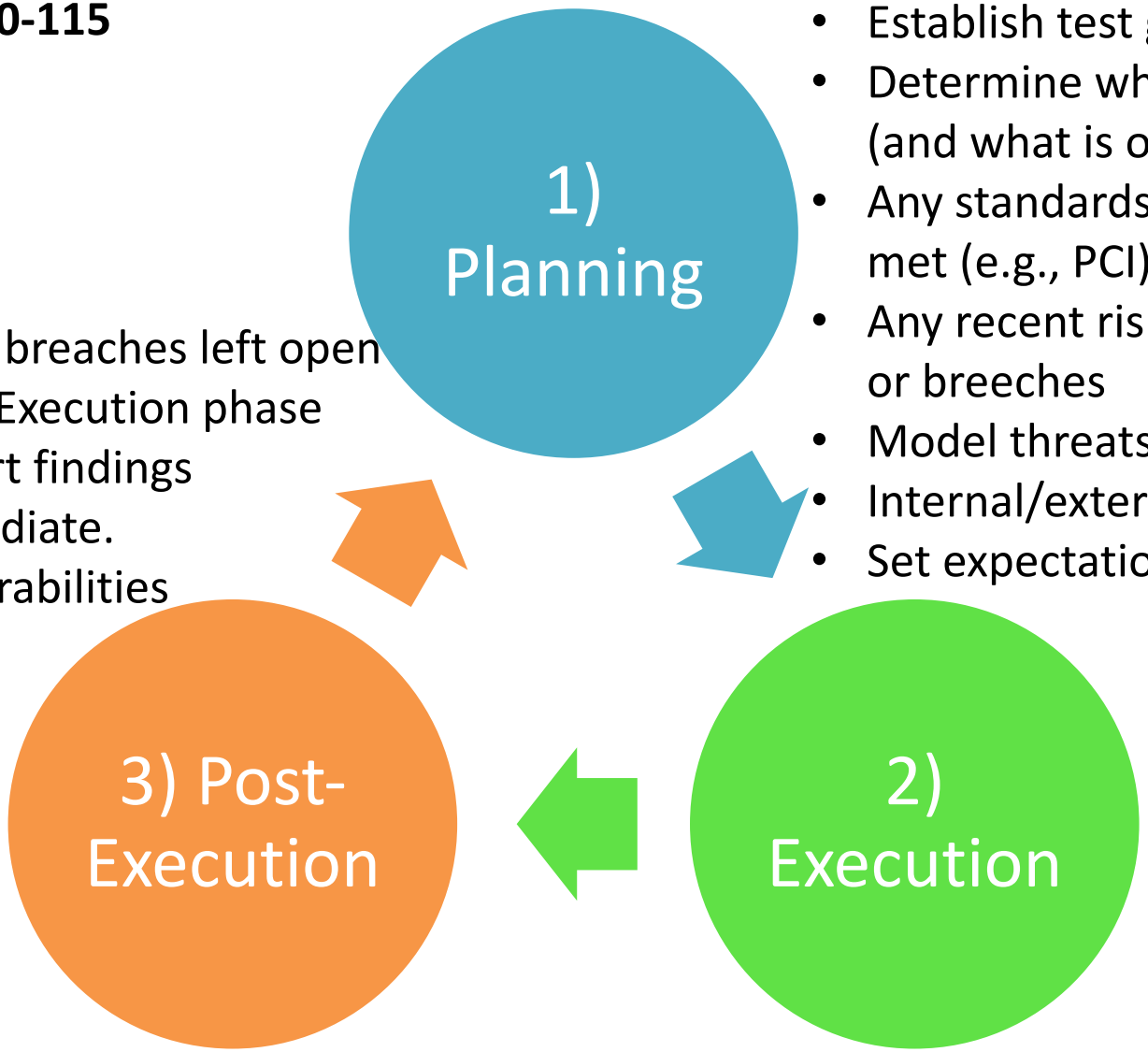
$2,450.00

View Details and Dates

Physical Intrusion Detection Systems: Practical Hacking and

Penetration testing typically involves three high-level phases

NIST 800-115



- Establish test goals/objectives
- Determine what will be tested (and what is off limits!)
- Any standards that must be met (e.g., PCI)
- Any recent risk analysis/audits or breeches
- Model threats
- Internal/external/red team
- Set expectations

- Intel gathering
- Network discovery
- Port and service identification
- Vulnerability scanning
- Wireless scanning

- Close breaches left open from Execution phase
- Report findings
- Remediate. vulnerabilities

Adapted from Scarfone, Karen A., et al. *SP 800-115. Technical Guide to Information Security Testing and Assessment*. 2008.

Example pen test process after planning phase; first external, then internal

- Port scan all 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, Vega, 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

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

Example pentest process after planning phase; first external, then internal

External

- Port scan all 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, Vega, 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

Goal: find what is vulnerable from over the Internet

Internal

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

Goal: find what is vulnerable from insiders

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