Welcome

Class Format

Professor Introduction

Lecture format

Tools we will use in the class

Syllabus Review

Code of Ethics Review and Vote

Student Introduction (What would you like to learn from this class?)

Professor Introduction

Who am I?

Information Security Professional /

Ethical Hacker / My Family

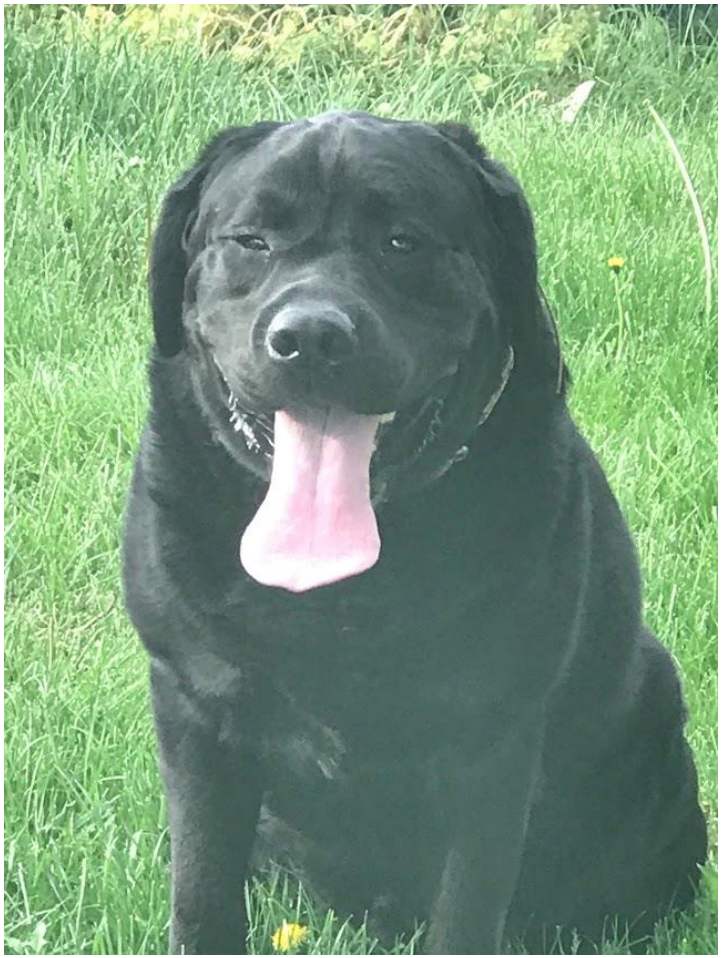
My Family

Height Difference

6’ 9”

6’ 4”

My Malcolm – Black English Lab



My Certifications

- My Certifications – A+, Security Plus, Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP) in process & Certified Cloud Security Professional (CCSP) in process

My Education

- Bachelor Degree – Drexel University
- Masters Degree – Arcadia University
- Ed.D in progress – Rowan University

Classes that I have taught

At Drexel University

Operating System Security Architecture I

Network Security

Information Technology Security II

Access Control and Intrusion Detection Technology

Operating Systems Architecture III

Senior Project I

Senior Project II

Security Technology Models and Architecture I

Computer Forensics II: Forensics and Investigations

IT Security Audits (CISA

At Arcadia University

I developed and taught Introduction to Information Security

At Rowan University

Network Management

Principles of Network Security

Jobs I've have/had

Rowan University, Glassboro, NJ

Manager of Information Security Architecture

Beneficial Bank, Philadelphia PA

VP of Information Security/Business Continuity Officer

Arcadia University, Glenside PA

Senior IT Security Risk and Compliance Analyst

Accume Partners, Moorestown, NJ

Senior Manager IT Security Auditor

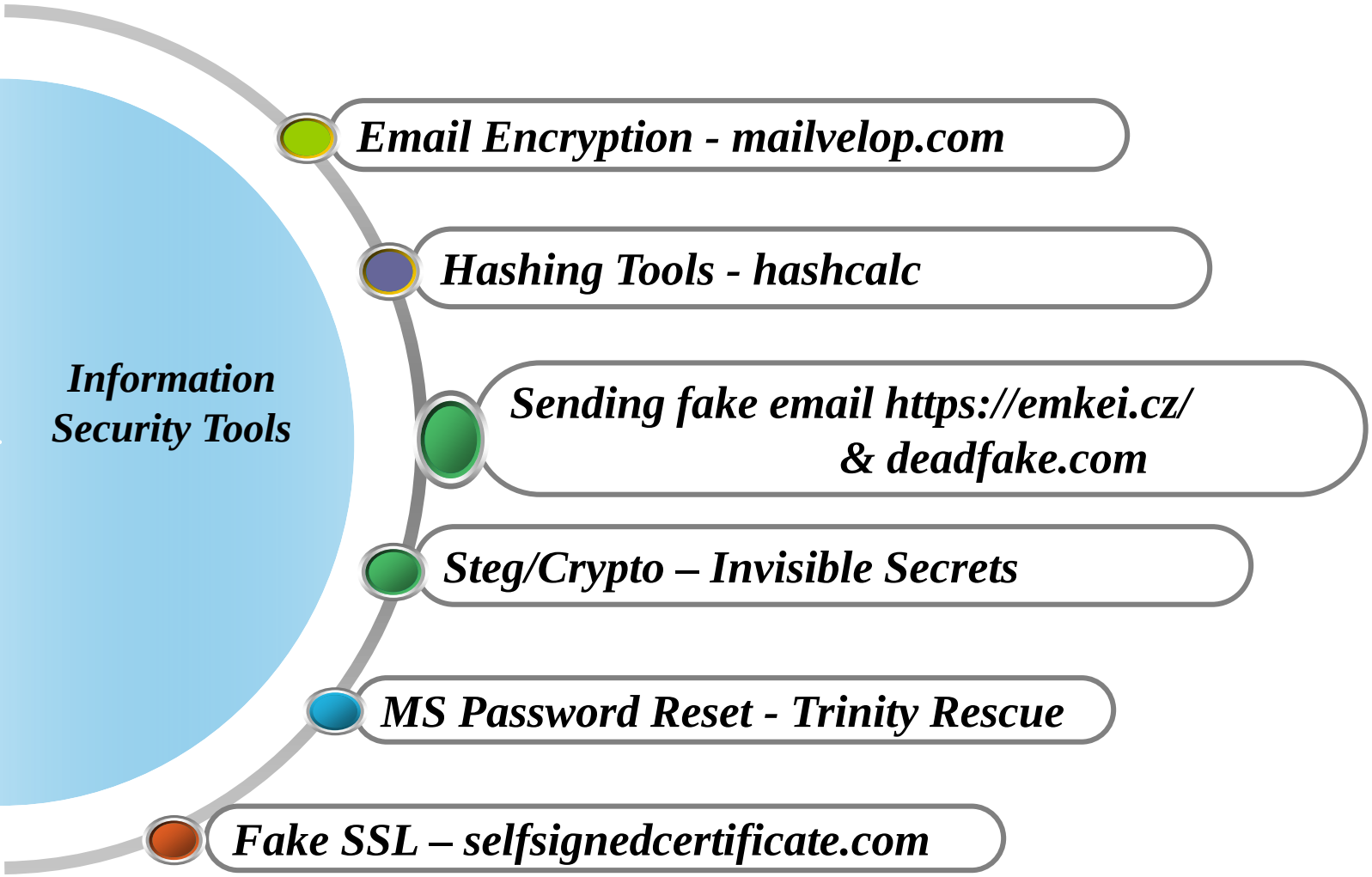
Lecture format –Please sign-in for every class (attendance will not be taken)

Teaching Styles

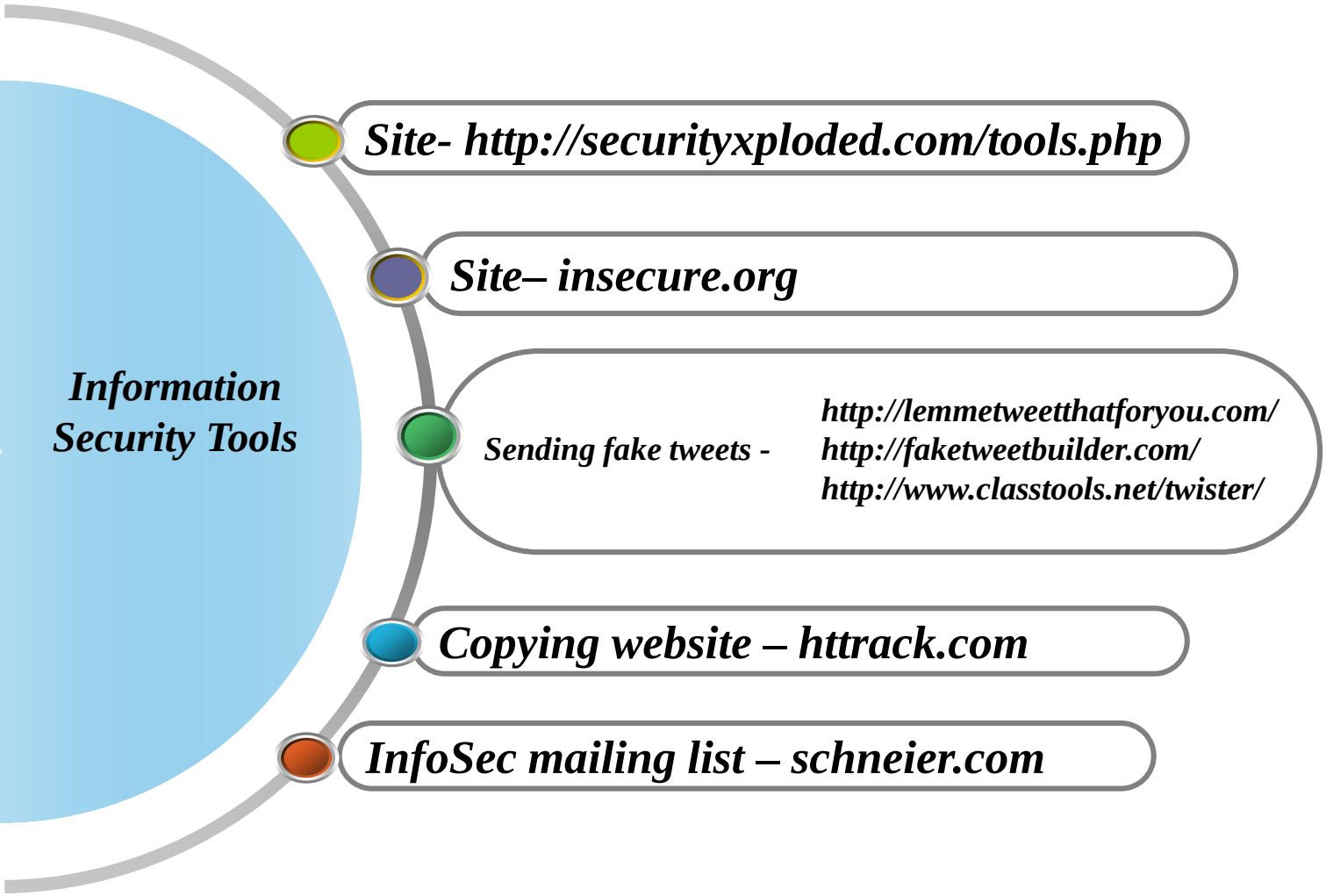
I teach real world experiences and issues

A NO STRESS LEARNING ENVIRONMENT

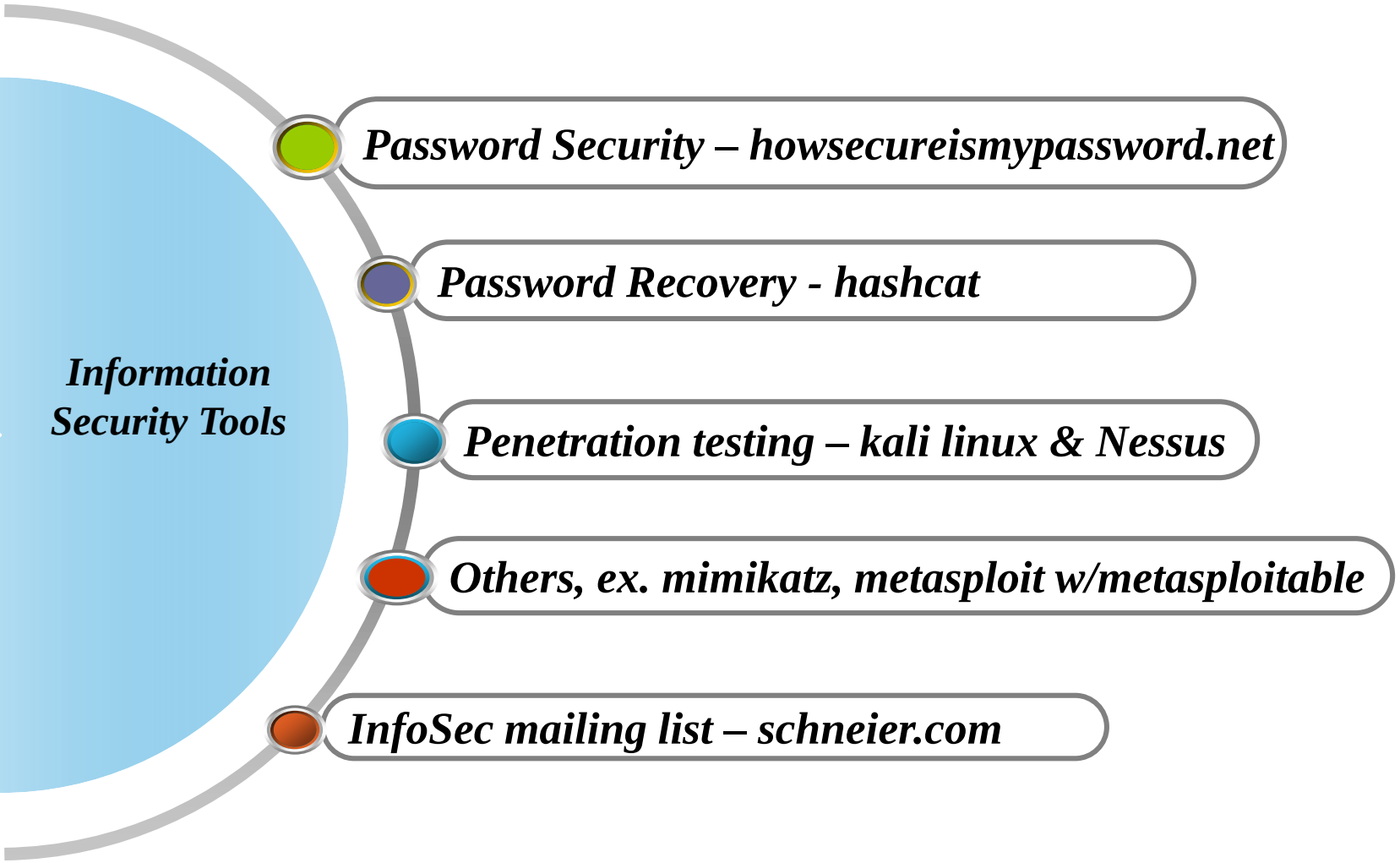
Information Security Tools we will use in this class



Information Security Tools we will use in this class



Information Security Tools we will use in this class



Networking/ Security Tools

- Network Simulations
- http://www.gns3.net/
- http://networksims.com/pix.html
- Network Traffic Generators
- https://iperf.fr/
- https://omnetpp.org/
- Other
- http://www.amanhardikar.com/mindmaps.html
- Hacking labs
- http://www.amanhardikar.com/mindmaps/Practice.html

Protect society, the commonwealth, and the infrastructure.

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally.

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service to principals.

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and protect the profession.

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

Thanks to ISC2 for allowing me to use some their ethics.

Lecture format – I am used to teaching this class once a week so I need the class to help me break at our appointed time.

Please sign-in for every class (attendance will not be taken)

Exams

All Exams will be completed via Blackboard and there will be no class on all Exam days.

Syllabus Review

End of the Semester
Project Review

Cybersecurity is understanding the importance of COMPUTER DECEPTION.

Hackers are always there doing what they do, and it’s our reasonability as Information Security Practitioners to locate them and be prepared for their tactics.

What is Information Security? It's the protection of data while keeping the data accessible to users.

Question??

Today, do you think we take Information Security Serious?

Let' see

http://www.privacyrights.org/data-breach

Why is Information So Important

- Let's look at some live Cyber Attacks
  - http://map.norsecorp.com/
  - https://geekflare.com/real-time-cyber-attacks/
  - http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17388&view=map
  - https://cybermap.kaspersky.com/

Great Websites for Cyber Security

- https://www.hackread.com/
- http://thehackernews.com/
- http://insecure.org/ (very helpful for project)
- http://www.kitploit.com/ (awesome info)

Student Introduction

Please tell us your name – then something about you – then what would you like to learn from this class?

As well as your

Technical Skills Assessment

Novice / Intermediate / Proficient

Team Assignment

5 Teams

Please start counting from 1-5, each number will determine your team designation

Team Code Names

1-Team Bot-BotNet

2- Team BackDoor

3-Team DoS

4-Team SQLInject

5-Team KeyLog

Team Responsibilities

Each team will perform all of their assigned tasked **either in class or remote**

1-Team Bot-BotNet –

Bot: A program that automates a usually simple action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. Like most things in the world of hacking, bots are, in themselves, benign and used for a host of legitimate purposes, like online content delivery. However, they are often used in conjunction with cracking, and that's where its public notoriety comes from. Bots can be used, for instance, to make the content calls that make up denial of service attacks. Bot is also a term used to refer to the individual hijacked computers that make up a botnet.

Botnet: A botnet is a group of computers controlled without their owners' knowledge and used to send spam or make denial of service attacks. Malware is used to hijack the individual computers, also known as "zombies," and send directions through them.

2-Team BackDoor –

Back door: A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections. Some have alleged that manufacturers have worked with government intelligence to build backdoors into their products. Malware is often designed to exploit back doors.

3-Team DoS –

Denial of service attack (DoS): DoS is used against a website or computer network to make it temporarily unresponsive. This is often achieved by sending so many content requests to the site that the server overloads. Content requests are the instructions sent, for instance, from your browser to a website that enables you to see the website in question. Some have described such attacks as the Internet equivalent of street protests and some groups, such as Anonymous frequently use it as a protest tool.

4-Team SQLInjection–

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

5-Team KeyLog–

KeyLogging is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

- Class Format
  - Lectures 60% - 80%
  - Exercises 10% - 20%

  Note: you will spend a considerable amount of time performing Exercises, please get to know your team members.

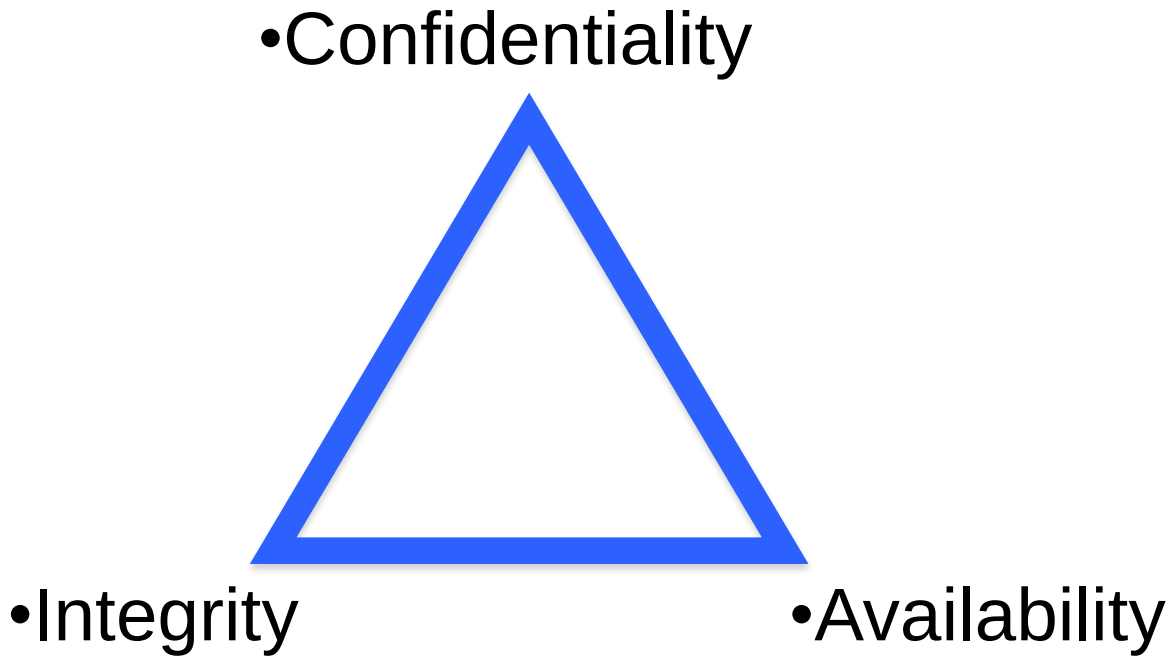
  All Exercises will be emailed, and each one will research the necessary objectives and complete the assignment.

Before we can get into Chapter 1, we must understand this

How safe is your password

- Quick Demo of Password Security
  - https://howsecureismypassword.net/
  - Other sites
    - Password Meter: http://www.passwordmeter.com/
    - Rumkin Strength Test: http://rumkin.com/tools/password/passchk.php
    - Test Your Password: http://www.testyourpassword.com/
    - Password Checker: http://password-checker.online-domain-tools.com/
    - Yet Another Password Meter: http://www.yetanotherpasswordmeter.com/
    - Microsoft Password Checker: https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx
    - Password Check: http://blog.kaspersky.com/password-check/
    - Intel's Password Game: https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html

The CIA of Security



The CIA of Computer Security

- Confidentiality
  - Preventing the disclosure of information to unauthorized persons.
- Integrity
  - The reliability of data. Authorization is necessary before data can be modified.
- Availability
  - Data is obtainable regardless of how information is stored, accessed, or protected.

Confidentiality

- Prevents unauthorized disclosure of data
- Ensures that data is only viewable by authorized users
  - Such as Personally Identifiable Information (PII)
- Some methods
  - Encryption
    - Ex: Advanced Encryption Standard (AES)
  - Access controls

Integrity

- Assures that data has not been modified, tampered with, or corrupted
- Only authorized users should modify data
- Hashing assures integrity
  - Hash types: MD5, SHA-1
  - If data changes, the hash value changes

Availability

- Data and services are available when needed
  - Remove SPOF (Single Point of Failure)

Availability

- Techniques:
  - Disk redundancies (RAID-redundant array of inexpensive)
  - Server redundancies (clusters)
  - Load balancing
  - Site redundancies
  - Backups
  - Alternate power (UPS, Backup Generator)
  - Cloud Services (Google Drive, Dropbox, etc.)

Hash Value for Download

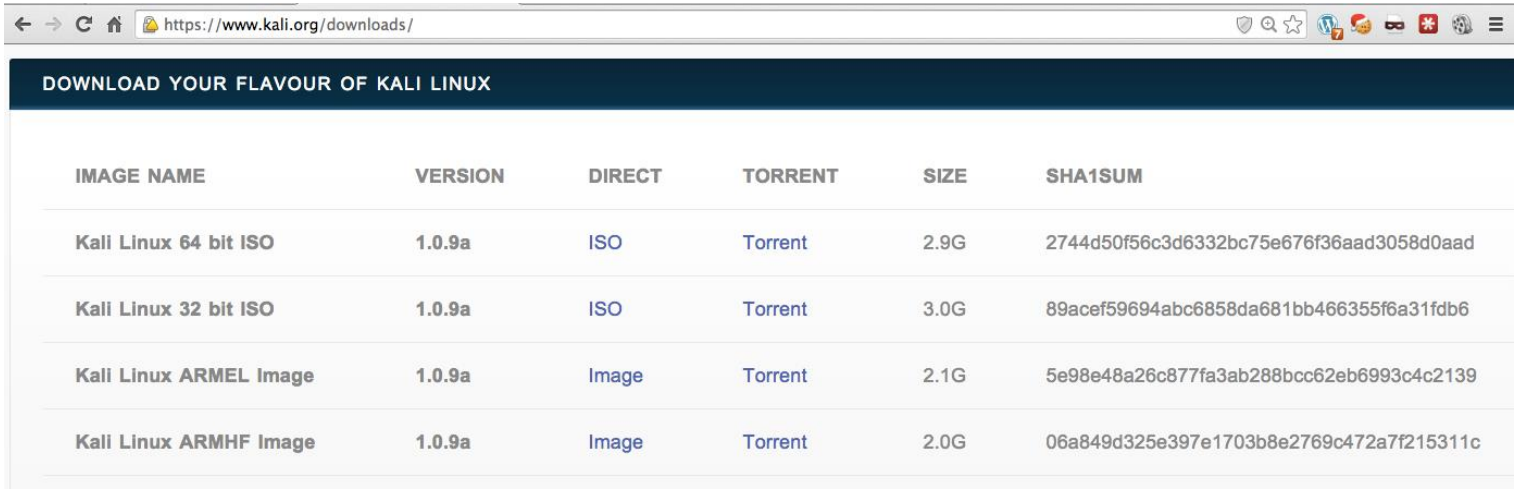


IMAGE NAME	VERSION	DIRECT	TORRENT	SIZE	SHA1SUM
Kali Linux 64 bit ISO	1.0.9a	ISO	Torrent	2.9G	2744d50f56c3d6332bc75e676f36aad3058d0aad
Kali Linux 32 bit ISO	1.0.9a	ISO	Torrent	3.0G	89acef59694abc6858da681bb466355f6a31fdb6
Kali Linux ARMEL Image	1.0.9a	Image	Torrent	2.1G	5e98e48a26c877fa3ab288bcc62eb6993c4c2139
Kali Linux ARMHF Image	1.0.9a	Image	Torrent	2.0G	06a849d325e397e1703b8e2769c472a7f215311c

Non-Repudiation

- Prevents entities from denying that they took an action
- Examples: signing a home loan, making a credit card purchase
- Techniques
  - Digital signatures
  - Audit logs-this too can be manipulated by an attacker

Access Controls

- Identification
  - Username: Who are you?
  - A claim, not proof
- Authentication
  - Proof of identity
  - Often by providing a password
- Authorization
  - Granting access to resources
- Accounting
  - Tracking of data, computer usage and network resources

Balancing CIA

- You can never have perfect security
- Increasing one item lowers others
- Increasing confidentiality generally lowers availability
  - Example: long ,complex passwords that are easily forgotten

  Each area will determine it's own level of security needs(C may be more important than I. or A and or vice-versa)

Patching

- Software requires frequent updates
- Patch Management
  - Testing patches to make sure they aren't harmful
  - Deploying them to all devices

Safety

- Safety of people
  - Escape plans and routes for fire, earthquake, etc.
  - Drills and training
- Safety of assets
  - Physical security controls
  - Fences, lighting, locks, CCTV (closed-circuit television) systems

Defense in Depth

- Layers of protection
- Example
  - Firewall (Using different vendors within your environment. Why one vulnerability will not compromise entire infrastructure.
  - Antivirus

- Network design
  - Understand network design elements such as hubs, switches, and routers, and how to protect those devices from attack.
  - Know network address translation, private versus public IP addresses, and the private IP ranges.
  - Create a solid foundation in network zones and interconnections, for example, intranets and extranets, demilitarized zones, LANs, and WANs.
  - Know how to defend against attacks on virtual local area networks, IP subnets, and telephony devices.
- Cloud security and server defense
  - Identify SaaS, IaaS, and PaaS, and know the pros and cons of using those services.
  - Understand the types of attacks against servers such as web, FTP, and email servers, and how to defend against them.

Network Devices

- Hub
  - A central connecting device used in a physical star topology
- Switch
  - Takes the place of hubs and bridges
  - Improves data transfer
  - *Type of attack:* MAC flooding
    - Sends numerous packets to a switch in an attempt to use all the switches memory
  - *Type of attack:* Physical tampering
- Router
  - Connects two or more networks to form an internetwork
  - Protect routers by using the following:
    - Firewalls
    - IPS
    - Secure VPN
    - Content filtering
    - ACLs

NAT and Private Versus Public IP

- Network Address Translation (NAT)
  - The process of changing an IP address while it is in transit across a router
- Private versus public IP addresses

IP Class	Assigned Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

1.0.0.0 - 9.255.255.255

11.x.x.x - 126.255.255.255

129.0.0.0 - 169.253.255.255

169.255.0.0 - 172.15.255.255

172.32.0.0 - 191.0.1.255

192.0.3.0 - 192.88.98.255

192.88.100.0 - 192.167.255.255

192.169.0.0 - 198.17.255.255

198.20.0.0 - 223.255.255.255

Network Zones, Interconnections and NAC

- Differences between LANs and WANs
  - LANs can be secured by using private IPs, using antimalware programs, and placing clients behind a router.
  - WAN connections should be monitored and firewalled to secure them.
- Internet and DMZs
  - A DMZ is a special area of the network (sometimes referred to as a subnetwork) that houses servers that host information accessed by clients or other networks on the Internet.
- Intranets and extranets
  - Enable access from remote employees or partner companies.
  - An intranet is generally when only one company is involved.
  - An extranet is generally when a second company is involved.
- Network Access Control (NAC)
  - Is a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.

Subnetting

- **Subnetting is the act of creating subnetworks logically through the manipulation of IP addresses.**
- **It is used to**
  - **Increase security by compartmentalizing the network.**
  - **Efficiently use IP address space.**
  - **Reduce broadcast traffic and collision**
- **Secure subnets by**
  - **Assigning different policies to each subnet**
  - **Updating routers**
  - **Monitoring all the subnets**

Virtual Local Area Networks (VLANs)

- VLANs
  - Implemented to segment the network, reduce collisions, organize the network, boost performance, and hopefully increase security
- VLAN hopping
  - Switch spoofing
    - Can be secured by placing unplugged ports into an unused VLAN, explicitly forwarding frames, and avoiding default VLAN names
  - Double tagging
    - Can be secured by upgrading firmware, utilizing an unused VLAN as the default, and redesigning the VLAN

Telephony Devices

- Modems
  - Secure by using the callback feature, using an authentication scheme, using modes sparingly, and keeping the number secret
- PBX
  - Secure by storing in a locked room, mounting the PBX, enabling only authorized maintenance, and monitoring remote ports
- VoIP
  - Reduce risk by updating the system and using encryption and authentication

Cloud Computing

- Understand the following cloud-based terms:
  - SaaS
  - IaaS
  - PaaS
  - Public cloud
  - Private cloud
  - Hybrid cloud
  - Community cloud

Cloud Security

- Understand the following cloud security methods:
  - Use complex passwords
  - Implement powerful authentication methods
  - Use strong cloud-based data access policies
  - Use encryption
  - Standardize programming methods
  - Protect all data

Server Defense

- Know how to protect file servers
  - Hardening
  - OS and application updates
  - Antimalware applications
  - Software-based firewalls
  - HIDS
  - Encryption
  - Monitor the server regularly
  - (This list applies to all servers!)

Server Defense (cont.)

- Understand how to protect network controllers and email servers
  - Prevent LDAP injection with proper input validation.
  - Prevent privilege escalation and spoofing by updating the OS.
  - Keep on top of the latest attacks.
  - Consider other technologies for email servers ex. Cloud based ex Gmail.

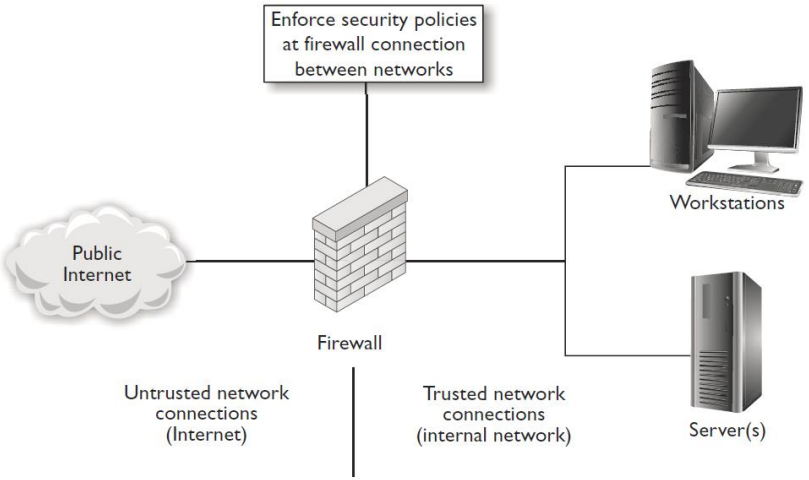
Server Defense (cont.)

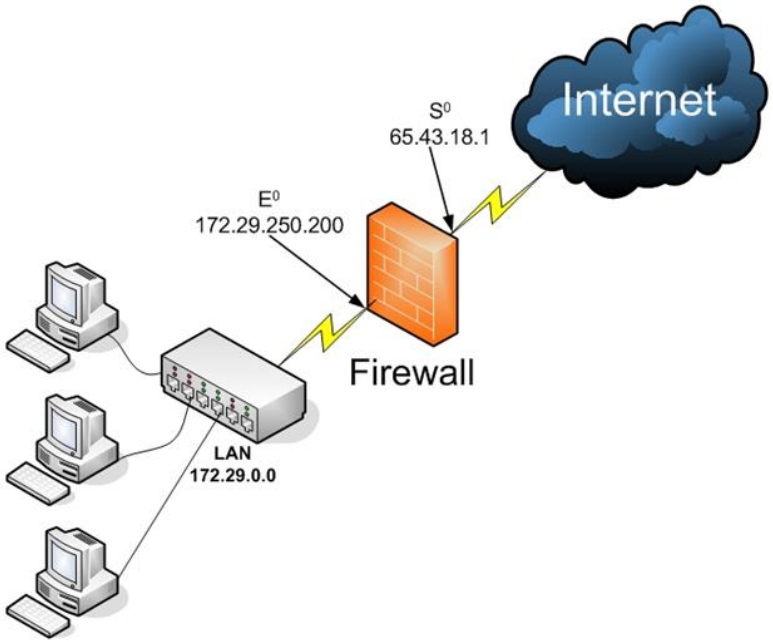
- Know how to protect web servers
  - Types of web servers include IIS, Apache, lighttpd, and so on, but they are all vulnerable to attack.
  - Keep up to date with security updates.
  - Stay informed of the latest Common Vulnerabilities and Exposures (CVE) maintained at:
    - http://cve.mitre.org
  - Apply patches quickly. (But test them first!)
  - Consider firewalls.
  - Use automated scanning programs Ex A/V.

Server Defense (cont.)

- Discuss how to protect FTP servers
  - Types of FTP servers include IIS's built-in FTP, Apache FtpServer, and FileZilla.
  - Consider secure FTP protocols such as FTPS or SFTP.
  - Use a dynamically assigned port for each file transfer instead of port 21 every time.
  - Use encryption.
  - Disable anonymous access (if at all possible).
    - Increase password security.
    - Change the admin passwords regularly.

Firewalls


Enforce security policies at firewall connection between networks
Public Internet
Firewall
Workstations
Server(s)
Untrusted network connections (Internet)
Trusted network connections (internal network)


Internet
S0
65.43.18.1
E0
172.29.250.200
Firewall
LAN
172.29.0.0

Firewalls cont.

- Personal software firewalls
  - Windows Firewall
  - Windows Firewall with Advanced Security
  - ZoneAlarm
  - Ipfirewall
  - iptables
- AV software firewalls
- Enterprise class firewalls Ex. Cisco ASA

Firewalls cont.

Packet filtering

Inspects each packet passing through the firewall and accepts or rejects it based on rules

N**AT filtering**

Filters traffic according to ports (TCP or UDP)

Application-level gateway

Applies security mechanisms to specific applications, such as FTP

Circuit-level gateway

Works at the session layer of the OSI model and applies security mechanisms when a TCP or UDP connection is established

MAC filtering

Filters out which computers can gain access to the firewall (and beyond) by their MAC address

IDS

- What is an IDS?
  - A device or software that monitors an individual computer system or a network, or portion of a network, and analyzes data that passes through to identify incidents and attacks.
  - IDS stands for intrusion detection system.
- Two main types of IDSs
  - Host-based intrusion detection system (HIDS)
  - Network intrusion detection system (NIDS)
- Two types of monitoring an IDS might use
  - Statistical anomaly
  - Signature-based
- Two types of misidentification
  - False positive
  - False negative
- Examples of IDS: Trend Micro OSSEC, Verisys, Tripwire

IDS/IPS

- **Same as IDS but with intelligence to re-act to issues in real time**

NIDS Versus NIPS

- Network intrusion detection system (NIDS)
  - A type of IDS that attempts to detect malicious network activities, for example port scans and DoS attacks.
- Network intrusion prevention system (NIPS)
  - Designed to inspect traffic, and based on its configuration or security policy, it can remove, detain, or redirect malicious traffic.
- The protocol analyzer's role
  - Protocol analyzers such as Wireshark (Ethereal) or Network Monitor are loaded on a computer and are controlled by the user in a GUI environment; they capture packets enabling the user to analyze them and view their contents.
  - Some NIDS and NIPS integrate these into their system.

Router

- Connects two or more networks to form an internetwork
- Protect routers by using the following:
  - Firewalls
  - IPS
  - Secure VPN
  - Content filtering
  - ACLs

Load Balancer

- Is a technique of load-balancing
- It distribute the processing load over two or more systems.
- It is great for resource utilization and throughput.

Proxies

- Takes requests from a client and forwards them to the destination system on behalf of the client
  - Anonymizing Proxy-keeps request anonymous
  - Caching Proxy-keeps local copy of all request, so when the request is made again the information is already available
  - Content filtering Proxy-checks all request and compares whether the request can be completed or denied
  - …
  - …

VPN/VPN Concentrators

- Technology that provides a secure communication between users across a public network ex. Internet
- It can encrypt either the data in the packet or encrypt the entire packet

Packet sniffer/Protocol Analyzer

- Software or Integrated Hardware/Software the captures and decode network traffic
- Most IDS/IPS is built using this technology
  - WireShark

Spam Filter

- A filter that block unsolicited or undesired emails
  - Blacklist list of servers known for sending spam
  - http://mxtoolbox.com/blacklists.aspx

Honeypots/Honeynets

Attract and trap potential attackers to counteract any attempts at unauthorized access of the network.

Honeypot

Generally a single computer but could also be a file, group of files, or an area of unused IP address space.

Honeynet

One or more computers, servers, or an area of a network; these are used when a single honeypot is not sufficient.

http://map.norsecorp.com/ or http://threatmap.fortiguard.com/ .

Honeypot software is usually not exactly easy to deploy and to configure, in order to simplify this process ThreatStream developed Modern Honey Network an open source

Unified Threat Management (UTM)

- A UTM is a combination of network security devices and methodologies including:
  - Firewalls
  - NIDS/NIPS
  - Content filtering
  - Antimalware systems
  - Data leak prevention
  - VPNs

Fun Fact

- What is the True Meaning of the Word "Hack?“
- http://www.secureworldexpo.com/what-true-meaning-word-hack