

Lesson 1.

Introduction to Information Security

Outline

1. What is Information Security?
2. Why is it important?
3. What can we do?
4. Security concepts
5. Practices: Ubuntu

What is Information Security?

Def 1:

Information security, often referred to as **InfoSec**, refers to the **processes** and **tools** designed and deployed to **protect sensitive business information** from **modification, disruption, destruction, and inspection**. (Ref: Cisco.com)

Def 2:

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

(Ref: wikipedia)

What is Information Security?

- The U.S. Government's [National Information Assurance Glossary](#) defines **INFOSEC** as:

*“Protection of information systems **against unauthorized access to or modification of information**, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.”*



What is Information Security?

- Three widely accepted elements or areas of focus (referred to as the “**CIA Triad**”):
 - Confidentiality
 - Integrity
 - Availability (Recoverability)
- Includes Physical Security as well as Electronic

Why is InfoSec Important?

- Information security is not an 'IT problem', it is a business issue.



Current ThreatScape Realities

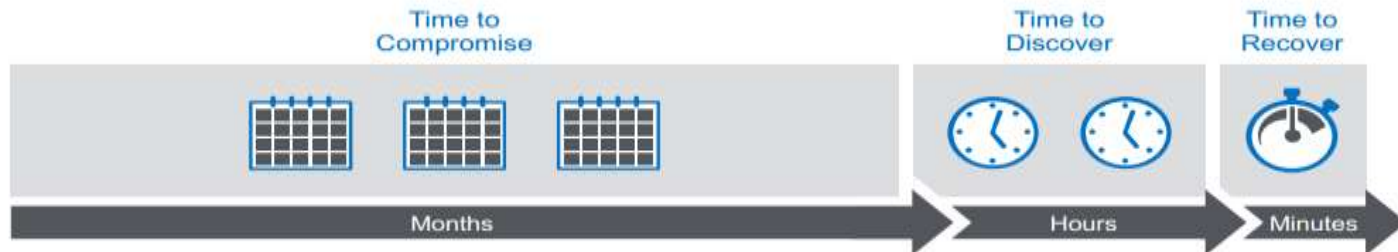


Minimal
Adversarial Effort

Overwhelmed
Security Teams

\$\$\$ Catastrophic
Impact \$\$\$

Business and Security Outcomes



Significant
Adversarial Effort

Optimized
Security Teams

\$ Minimized
Impact \$

Main goals of Information Security

- **Confidentiality:** only authorized entities have access to the data
- **Integrity:** there are no unauthorized modifications of the data
- **Availability:** authorized entities can access the data when and how they are permitted to do so



(C-I-A Triad)

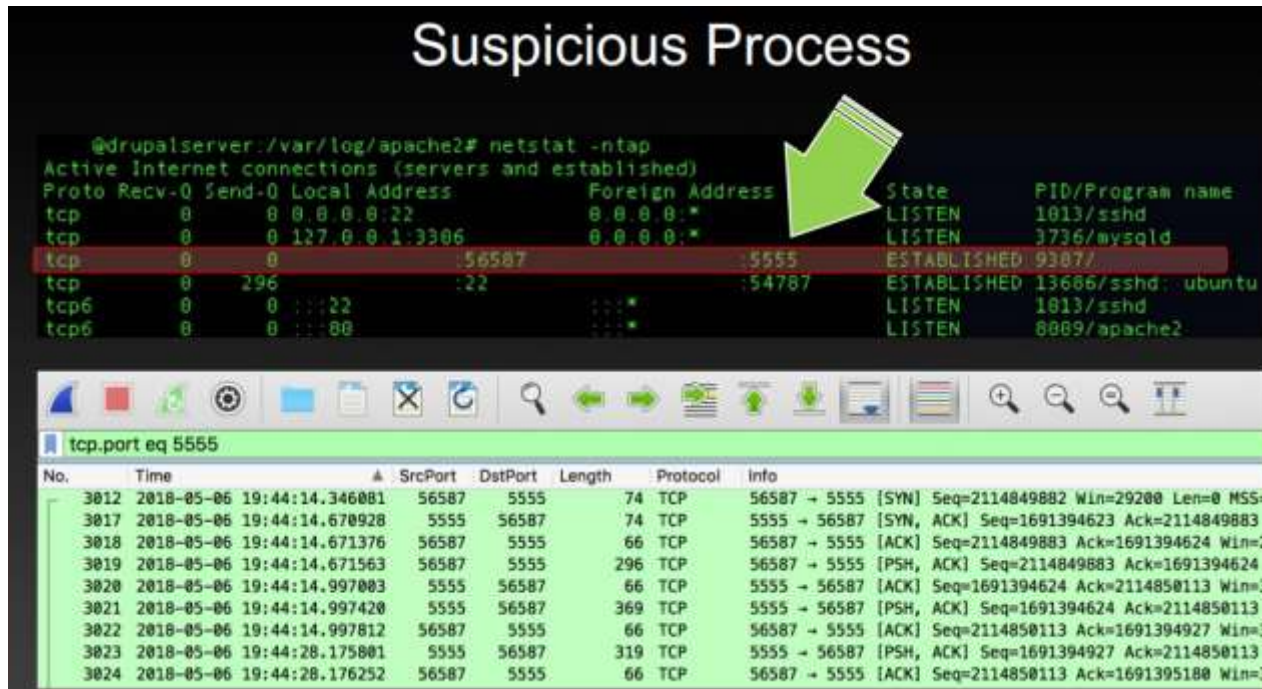
What can we do?

- **Security Assessment**
 - Identify areas of risk
 - Identify potential for security breaches, collapses
 - Identify steps to mitigate
- **Security Application**
 - Expert knowledge (train, hire, other)
 - Multi-layered Approach (there is no single solution)
 - Policies and Procedures

What can we do?

- **Security Awareness**
 - Not just for the geeks!
 - Security Training at all levels (external and/or internal)
 - Continuing education and awareness – not a one-time shot!
 - Make it part of the culture

Suspicious Process

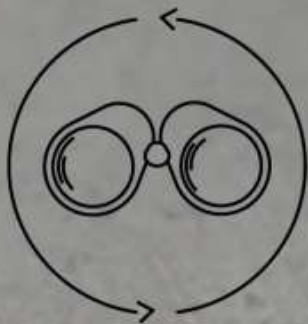


```
@drupalserver:/var/log/apache2# netstat -ntap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1013/sshd
tcp        0      0 0.0.0.0:5555            0.0.0.0:*               LISTEN      9307/
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      3736/mysqld
tcp        0      0 0.0.0.0:5555            0.0.0.0:*               ESTABLISHED 13686/ssh: ubuntu
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1013/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      1013/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      8889/apache2
```

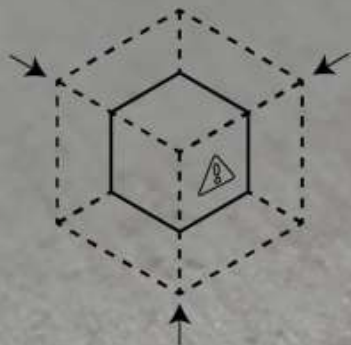
tcp.port eq 5555

No.	Time	SrcPort	DstPort	Length	Protocol	Info
3012	2018-05-06 19:44:14.346081	56587	5555	74	TCP	56587 → 5555 [SYN] Seq=2114849882 Win=29200 Len=0 MSS=
3017	2018-05-06 19:44:14.670928	5555	56587	74	TCP	5555 → 56587 [SYN, ACK] Seq=1691394623 Ack=2114849883
3018	2018-05-06 19:44:14.671376	56587	5555	66	TCP	56587 → 5555 [ACK] Seq=2114849883 Ack=1691394624 Win=2
3019	2018-05-06 19:44:14.671563	56587	5555	296	TCP	56587 → 5555 [PSH, ACK] Seq=2114849883 Ack=1691394624
3020	2018-05-06 19:44:14.997003	5555	56587	66	TCP	5555 → 56587 [ACK] Seq=1691394624 Ack=2114850113 Win=3
3021	2018-05-06 19:44:14.997420	5555	56587	369	TCP	5555 → 56587 [PSH, ACK] Seq=1691394624 Ack=2114850113
3022	2018-05-06 19:44:14.997812	56587	5555	66	TCP	56587 → 5555 [ACK] Seq=2114850113 Ack=1691394927 Win=3
3023	2018-05-06 19:44:28.175801	5555	56587	319	TCP	5555 → 56587 [PSH, ACK] Seq=1691394927 Ack=2114850113
3024	2018-05-06 19:44:28.176252	56587	5555	66	TCP	56587 → 5555 [ACK] Seq=2114850113 Ack=1691395100 Win=3

What can we do?



**COMPLETE
VISIBILITY**



**REDUCE
ATTACK
SURFACE**



**PREVENT
KNOWN
THREATS**



**PREVENT
UNKNOWN
THREATS**



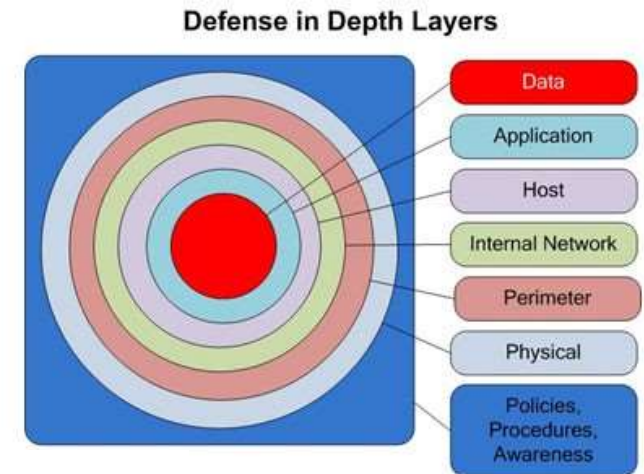
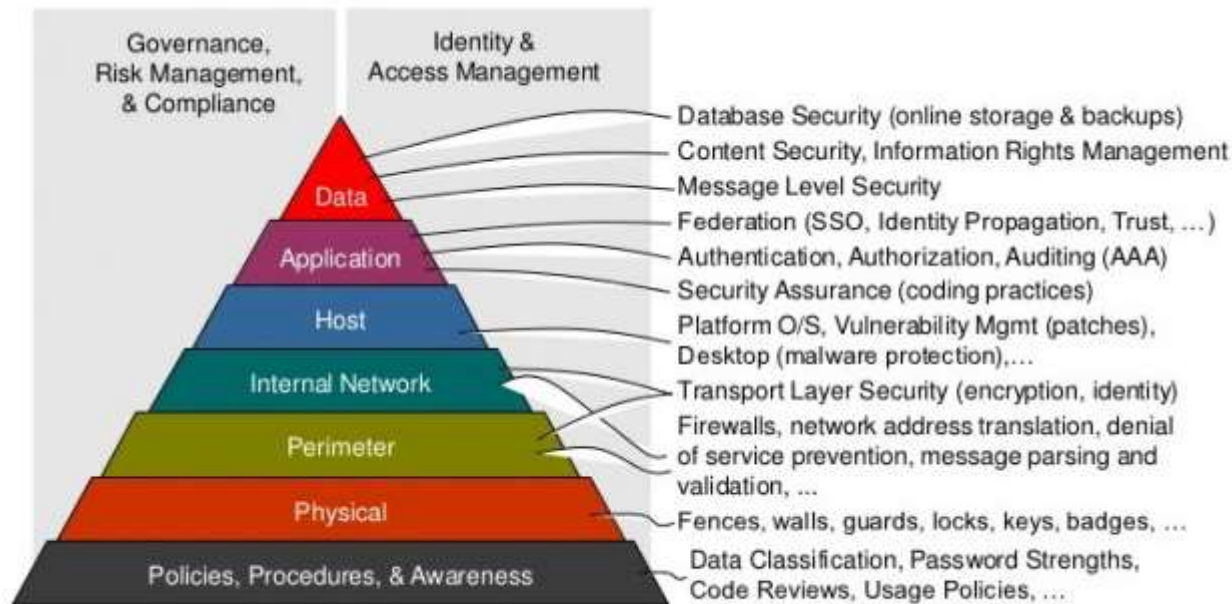
paloalto
NETWORKS

Principle of Least Privilege

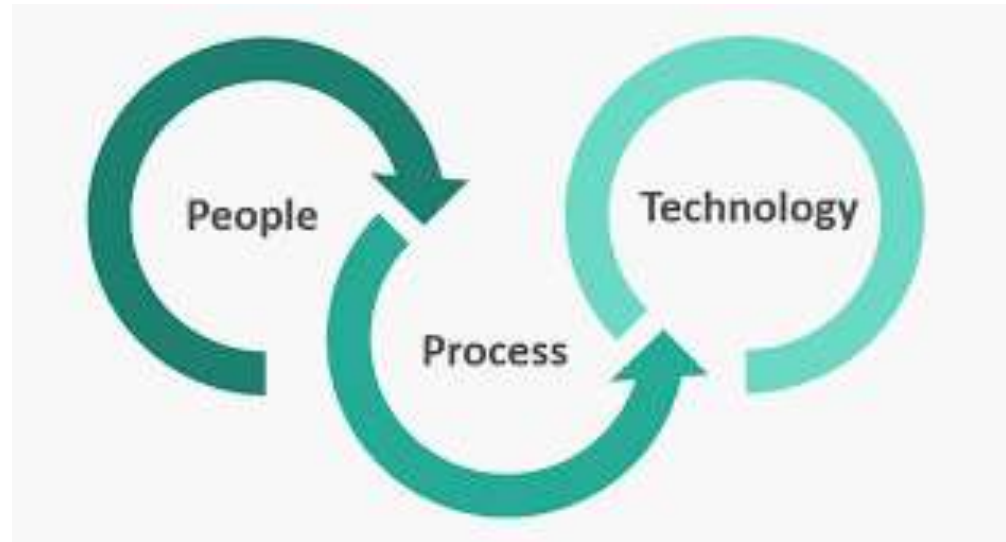
- Every program and every privileged user of the system should operate using the least amount of privileges necessary to complete the job

What can we do?

- Defense in depth



What can we do?



Cyber-security is not just about technology, IT or engineers.

C-I-A

- Confidentiality
- Integrity
- Availability

P-P-T

- People
- Process
- Technology

Governance

- Policy
- Audit
- Awareness

Security Concepts

- Authentication
- Authorization
- Accounting
- Access control
- Nonrepudiation
 - The ability to ensure that someone cannot deny his/her actions



Security Control Frameworks

- This is a notional construct outlining the organization's approach to security, including a list of specific security processes, procedures, and solutions used by the organization. Some frameworks:
 - ISO 27001/27002
 - COBIT
 - ITIL
 - RMF
 - CSA STAR

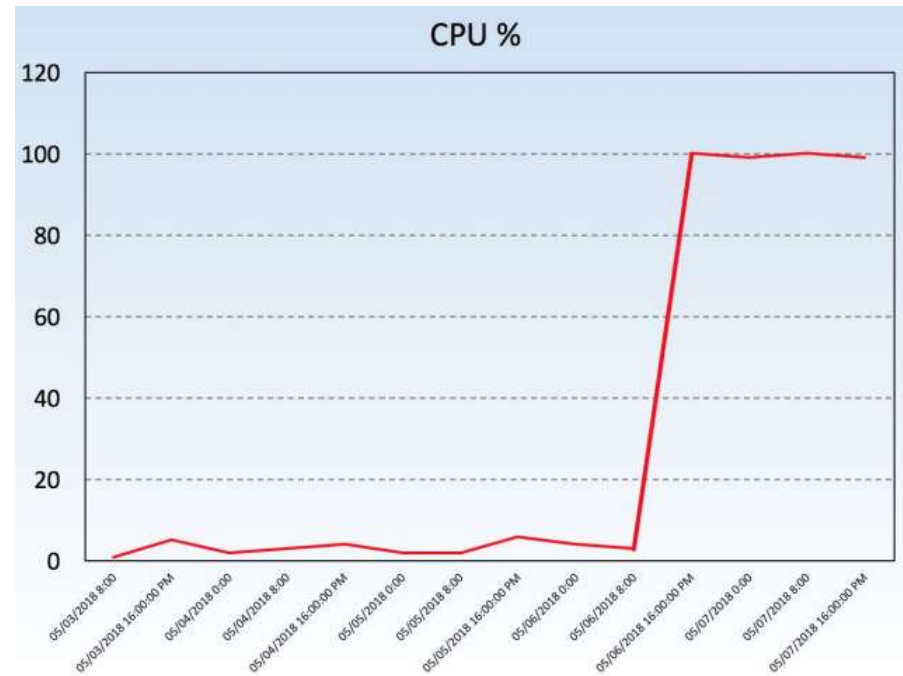
Practices

- OS: Ubuntu 16.04 (32 bit)
- Some commands:
 - cd
 - ls
 - cp
 - mkdir
 - chown
 - Chmod
 - ...
- Software:
 - C: gcc -o exploit exploit.c

Summary

- Objective of InfoSec is ***Confidentiality, Integrity and Availability***...protect your systems and your data
- Threats are numerous, evolving, and their impact is costly
- Security should be applied in layers (“road blocks”)
- Security Awareness at all levels must be maintained
- Practices: Ubuntu (cd, ls, mkdir, chmod, chown,...)

Q&A



Add Filter				All Devices	Custom...	May 02 To May 07
#	Threat	Category	Threat Level			
1	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	IPS	Critical			
2	Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	IPS	Critical			
3	MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	IPS: CVE-2017-7269	Critical			
4	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	IPS	Critical			
5	Linksys.Routers.Administrative.Console.Authentication.Bypass	IPS	High			
6	Proxy.HTTP	Proxy	Medium			
7	D-Link.DIR.800.Series.getcfg.php.Information.Disclosure	IPS	Medium			
8	Failed Connection Attempts	Failed Connection Attempts	Low			
9	ZmEu.Vulnerability.Scanner	IPS	Low			
10	Masscan.Scanner	IPS	Low			

Questions (MQCs)

Q1. Messagemeans that the data must arrive at the receiver exactly as sent

- A. Confidentiality
- B. Integrity
- C. Authentication
- D. None of the above

Answer: B

Q2. Cryptography does not concern itself with:

- A. Availability
- B. Authenticity
- C. Integrity
- D. Confidentiality

Answer: A

Q3. An access control system that grants users only those rights necessary for them to perform their work is operating on **which security principle?**

- A. Discretionary Access
- B. Least Privilege
- C. Mandatory Access
- D. Separation of Duties

Answer: B

Q4. Which of the following is the verification of a person's identity?

- A. Authorization
- B. Accoutability
- C. Authentication
- D. Password

Answer: C

Q5. John is concerned about social engineering. He is particularly concerned that this technique could be used by an attacker to obtain information about the network, including possibly even passwords. What countermeasure would be most effective in combating social engineering?

- A. SPI firewall
- B. An IPS
- C. User training
- D. Strong policies

Answer: C

Q6. The application of which of the following standards would BEST reduce the potential for data breaches?

- A. ISO 9000
- B. ISO 20121
- C. ISO 26000
- D. ISO 27001

Answer: D

Q7. The first phase of hacking an IT system is compromise of which foundation of security?

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Authentication

Answer: B

Q8. The PRIMARY purpose of a security awareness program is to?

- A. Ensure that everyone understands the organization's policies and procedures.
- B. Communicate that access to information will be granted on a need-to-know basis.
- C. Warn all users that access to all systems will be monitored on a daily basis.
- D. Comply with regulations related to data and information protection.

Answer: A

Q9. Which type of cyber attack is commonly performed through emails?

A. Trojans

B. Phishing

C. Worms

D. Ransomware

Answer: B

Q10. The use of strong authentication, the encryption of Personally Identifiable Information (PII) on database servers, application security reviews, and the encryption of data transmitted across networks provide

- A. Data integrity.
- B. Defense in depth.
- C. Data availability.
- D. Non-repudiation.

Answer: B