February 9, 2021
Intrusion Protection

COLLEGE of CHARLESTON 1770

- Changes
  - Syllabus
- Today
  - Authentication
  - Security Orchestration
  - Intrusion Detection
- Assignments
  - Lab 1: Due Monday, Feb 22
  - Project
    - Topic Due: Monday, Feb 22

Authentication

- Passwords
  - Internal (imbedded in code)
  - External (user)
- Other approaches?

difficulty

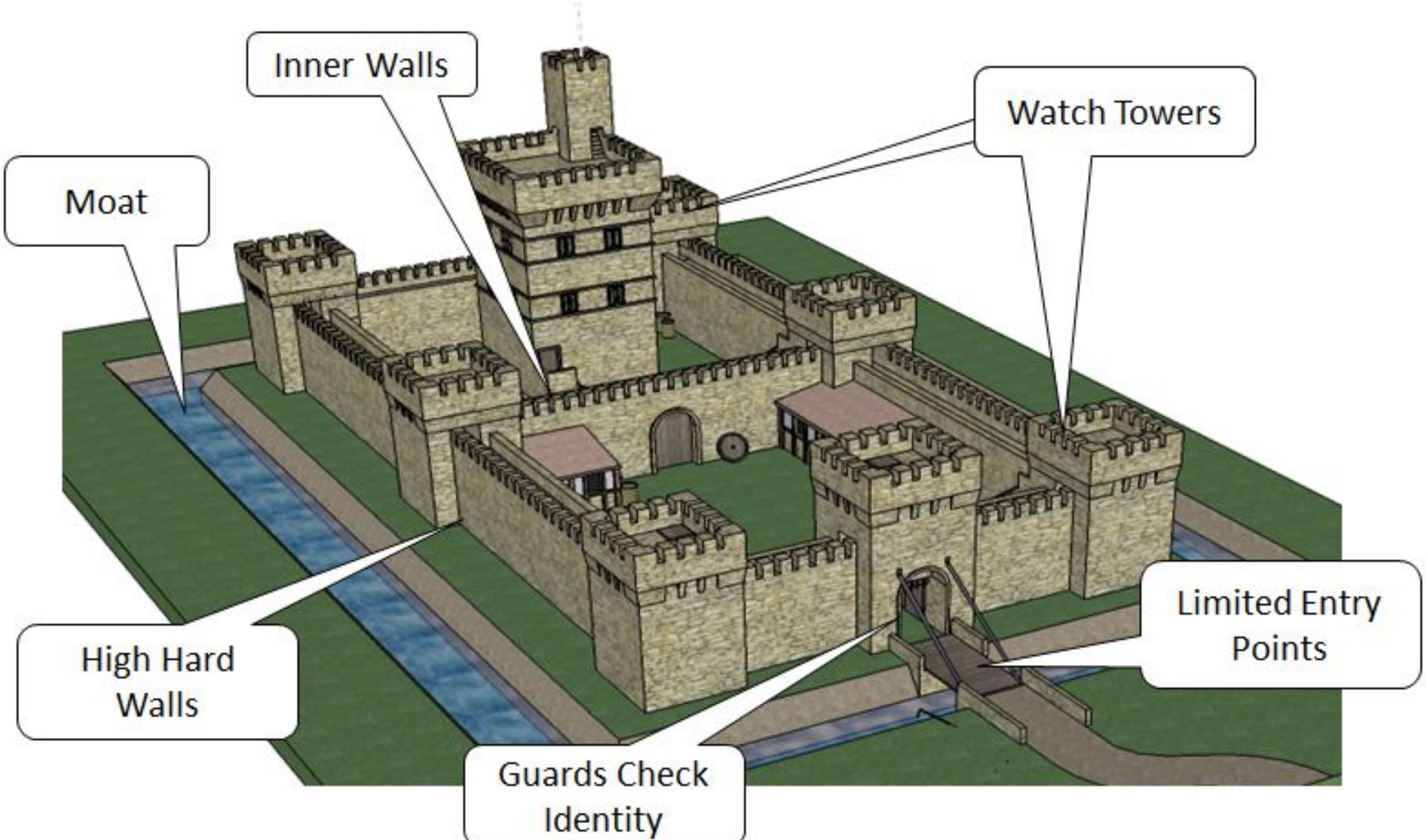
- ENV file
- environment variables
- hashing
- public key authentication
- certificates

Finding security exposures

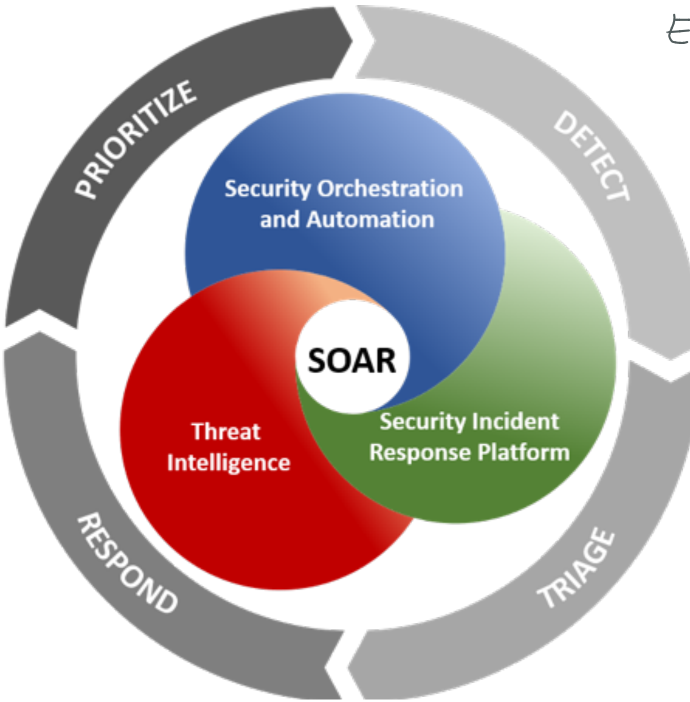
- Source code scanning
- Pen testing tools

DevOps

- Devopment ⟷ Operations
- Automation


Inner Walls
Watch Towers
Moat
High Hard Walls
Limited Entry Points
Guards Check Identity

Security Orchestration, Automation and Response (SOAR)



Splunk
ELASTIC SEARCH
↳ kibana
↳ graphana

Network Intrusion Detection Systems (NIDSs)

- Authorized eavesdropper that listens in on network traffic
- Makes determination whether traffic contains malware
  - usually compares payload to virus/worm signatures
  - usually looks at only incoming traffic
- If malware is detected, IDS somehow raises an alert
- Intrusion detection is a **classification problem**

ALTERNATIVE IS
REGRESSION Problem

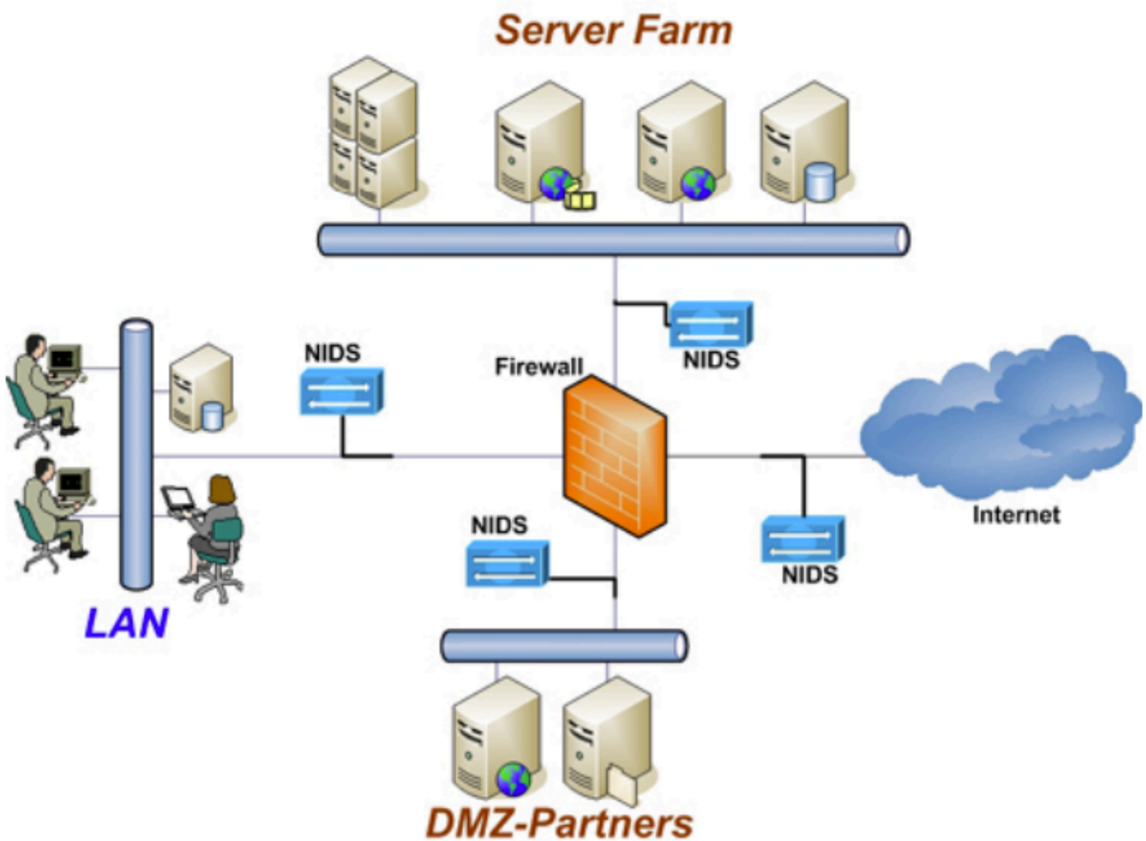
Host Intrusion Detection Systems (HIDSs)

- Intrusion detection that takes place on a single host system.
- Agent monitors and reports on
  - system configuration
  - application activity
- log analysis, event correlation, integrity checking, policy enforcement, rootkit detection, and alerting[1]. They often also have the ability to baseline a host system to detect variations in system configuration. In specific vendor implementations these HIDS agents also allow connectivity to other security systems.

HIDS and Antivirus

- Are they the same?
- Do they have differences?
- Do they have overlap?

HIDS is a superset
Antivirus is part of
HIDS

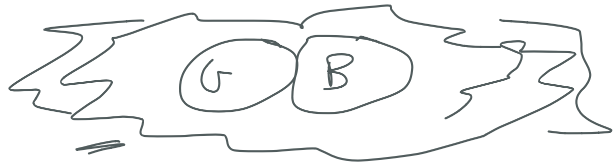

Server Farm
NIDS
Firewall
NIDS
Internet
NIDS
NIDS
LAN
DMZ-Partners

Detection via Signatures

- Signature checking: does packet match some signature?
  - Payload, e.g., shellcode
  - Header, e.g., SYN
- Problem: not so great for zero-day attacks -- Q: WHY?

- NORMAL patterns of activity
- Can be difficult to track

Detection via Machine Learning



- Underlying assumption:
  - Malware will look different from non-malware
  - Anomaly in traffic will look different than regular traffic
- Supervised Learning:
  - IDS requires learning phase in which operator provides pre-classified ***training data*** to learn patterns
  - Sometimes called **anomaly detection (systems)**
  - {good, 80, “GET”, “/”, “Firefox”}
  - {bad, 80, “POST”, “/php-shell.php?cmd=’rm -rf /’”, “Evil Browser”}
  - ML technique builds model for classifying never-before-seen packets
  - Problem: is new malware going to look like training malware?

Metrics

- **True positives** (TP): number of correct classifications of malware/anomaly
- **True negatives** (TN): number of correct classifications of non-malware/regular
- **False positives** (FP): number of incorrect classifications of non-malware as malware/anomaly
- **False negatives** (FN): number of incorrect classifications of malware as non-malware/regular

Metrics

- **False positive rate**:
$$FPR = \frac{FP}{FP+TN} = \frac{\#benign\_marked\_as\_malicious}{\#total\_benign}$$
- **True negative rate**: $\frac{\text{TN} \leftarrow \text{DETECTED}}{\text{TOTAL NEGATIVES}}$
- **False negative rate:**
- **True positive rate:**

Base Rate Fallacy

- Occurs when we assess $P(X|Y)$ without considering prior probability of X and the total probability of Y
- Example:
  - *Base rate* of malware is 1 packet in a 10,000
  - Intrusion detection system is 99% accurate (given known samples)
    - 1% false positive rate (benign marked as malicious 1% of the time)
    - 1% false negative rate (malicious marked as benign 1% of the time)
  - Packet X is marked by the NIDS as malware. *What is the probability that packet X actually is malware?*
    - Let's call this the "true alarm rate," because it is the rate at which the raised alarm is actually true.

Probability and Bayes' Rule

- Pr(*x*) function, probability of event *x*
  - Pr(sunny) = .8 (80% of sunny day)
- Pr(x|y), probability of x given y
  - Conditional probability
  - Pr(cavity|toothache) = .6
  - 60% chance of cavity given you have a toothache

Probability and Bayes' Rule

- Bayes' Rule (of conditional probability):

$$\Pr(D|\theta)\Pr(D) = \Pr(\theta|D)\,\Pr(\theta)$$

$$\Pr(D|\theta) = \frac{\Pr(\theta|D)\,\Pr(\theta)}{\Pr(D)}$$

- Assume:
  - Pr(cavity|toothache) = .6
  - Pr(cavity) = .5
  - Pr(toothache) = .1
- What is Pr(toothache|cavity)?

$\frac{.6 \cdot .1}{.5} = .12$

Base Rate Fallacy

- How do we find a true alarm rate?
  Pr(Is Malware | Marked As Malware)
- We know:
  - 1% false positive rate (benign marked as malicious 1% of the time); True negative rate= 99%
  - 1% false negative rate (malicious marked as benign 1% of the time); True Positive Rate= 99%
  - *Base rate* of malware is 1 packet in 10,000
- What is?
  - Pr(MarkedAsMalware|IsMalware) = 0.99
  - Pr(IsMalware) = 0.0001
  - Pr(MarkedAsMalware) = 0.01

Base Rate Fallacy

- How do we find the true alarm rate? Pr(IsMalware|MarkedAsMalware)

$$Pr(IsMalware|MarkedAsMalware) = \frac{Pr(MarkedAsMalware|IsMalware) \cdot Pr(IsMalware)}{Pr(MarkedAsMalware)}$$

$$= \frac{0.99 \cdot 0.0001}{0.01} = 0.0099$$

- Therefore, *only about 1% of alarms are actually malware!*
  - What does this mean for network administrators?

Base Rate Fallacy Summary

- Let Pr(M) be the probability that a packet is actually malware (thebaserate)
- Let Pr(A) be the probability that the IDS raises an alarm (unknown)
- Assume we also know for the IDS
  - Pr(A|M)=TPR=1-FNR
  - Pr(A|!M)=FPR
- $$Pr(M|A) = \frac{Pr(A|M) \cdot Pr(M)}{Pr(A|M) \cdot Pr(M) + Pr(A|!M) \cdot Pr(!M)}$$

Where is Anomaly Detection useful?

System	Intrusion Density P(M)	Detector Alarm Pr(A)	Detector Accuracy Pr(A|M)	True Alarm P(M|A)
A	0.1	0.38	0.65	0.171
B	0.001	0.01098	0.99	$\boxed{0.090164}$
C	0.1	0.108	0.99	0.911667
D	0.00001	0.00002	0.99999	0.5

Problems with IDSs

- VERY difficult to get both good recall and precision
- Malware comes in small packages
- Looking for one packet in a million (billion? trillion?)
- If insufficiently sensitive, IDS will miss this packet (low recall)
- If overly sensitive, too many alerts will be raised (low precision)

Snort

- Open source IDS
- Signature detection
- Lots of available rulesets
- alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 3306 (msg:"MYSQL root login attempt"; flow:to_server,established; content:"|0A 00 00 01 85 04 00 00 80|root|00|"; classtype:protocol-command-decode; sid:1775; rev:2;)