



PWNING MACHINE LEARNING SYSTEMS



**TIME TO
INSTALL DA VM**

AGENDA - PART 1

10min INTRO + SETUP

30min ML CRASH COURSE

30min ML IDS/WAF PLAY TIME

40min ML IDS/WAF POISONING

10min BREAK

AGENDA - PART 2

20min DEEP LEARNING PRIMER

30min PWINING DEEP LEARNING SYSTEMS

30min SPEAR PHISHING WITH DEEP LEARNING

40min SECRET PROJECT ;)

Let f be a function representing this training session.
Let x be the amount of math involved.

$$\lim_{x \rightarrow 0} f(x)$$

OUR TOOLZ

- **scikit-learn** - implements a range of machine learning algorithms
- **TensorFlow** - library for numerical computation using flow graphs / deep learning

SCIKIT-LEARN

- easy-to-use, general-purpose toolbox for machine learning in Python.
- supervised and unsupervised machine learning techniques.
- Utilities for common tasks such as model selection, feature extraction, and feature selection
- Built on NumPy, SciPy, and matplotlib
- Open source, commercially usable - BSD license

TENSORFLOW

- Open source, originally Google Brain
- Widely used in both research and production
- Main popular use is for deep learning/neural nets
 - But not restricted to just deep models
- Multiple GPU Support

YOU NEED THESE



NumPy

Base N-dimensional
array package



SciPy library

Fundamental
library for scientific
computing



Matplotlib

Comprehensive 2D
Plotting

IP[y]:
IPython

IPython

Enhanced
Interactive Console



Sympy

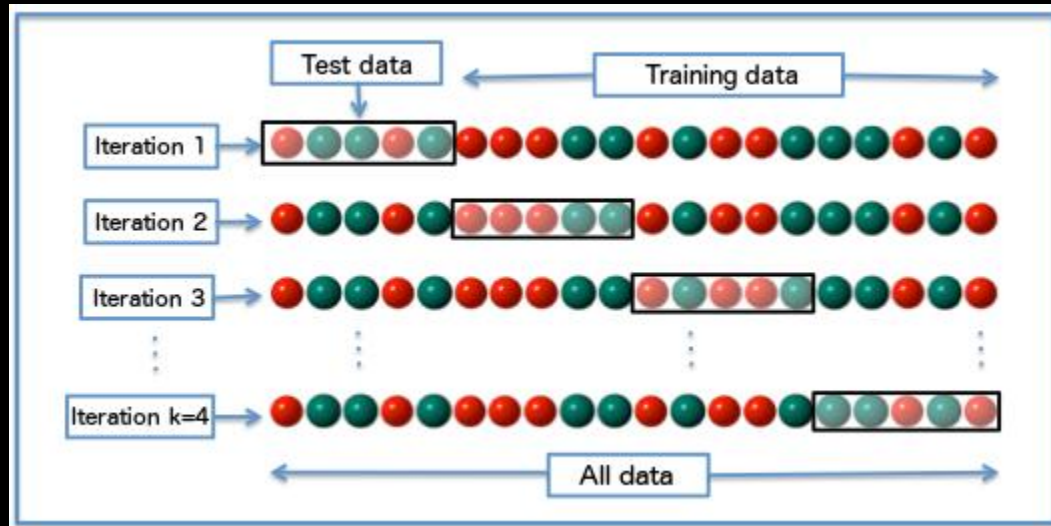
Symbolic
mathematics



pandas

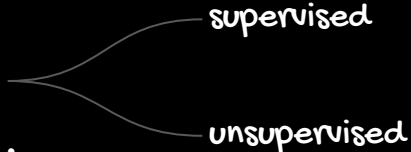
Data structures &
analysis

CROSS VALIDATION



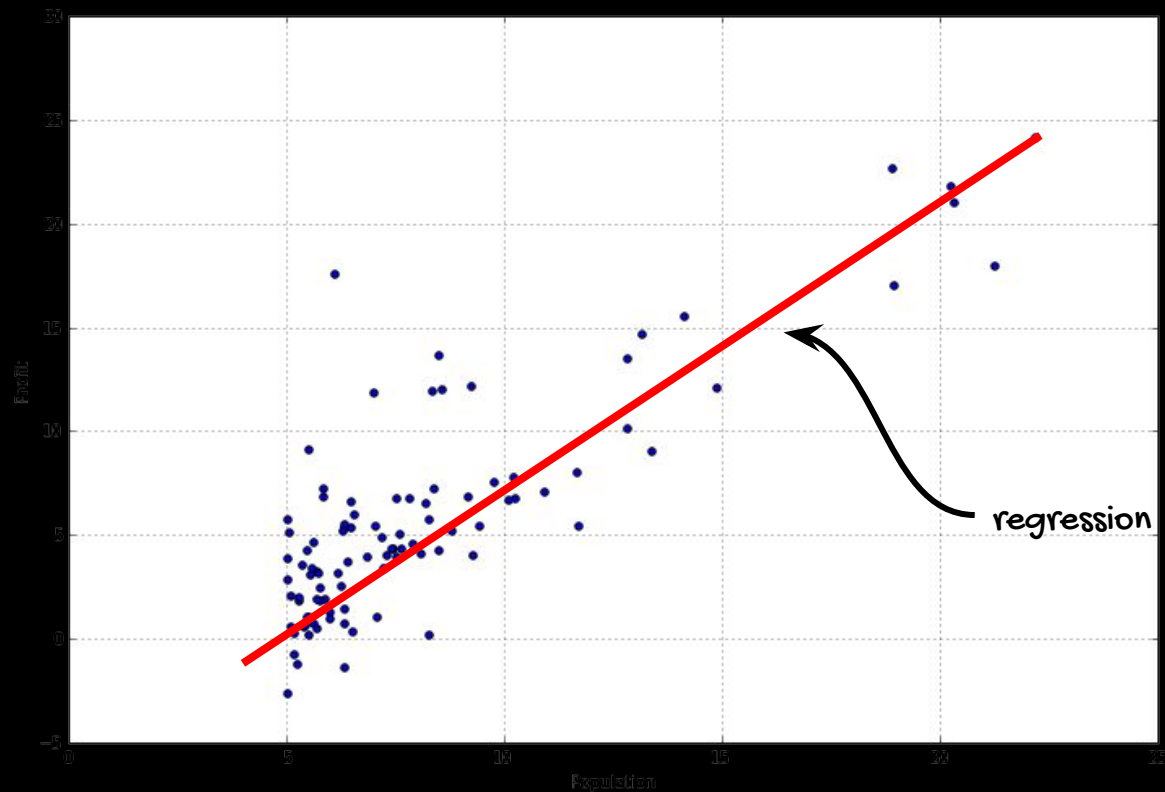
MACHINE LEARNING 101

Types of machine learning use cases:

- Regression
 - Classification
 - Anomaly detection
 - Recommendation
- won't cover here, but check out [this talk](#)
- 
- The diagram shows two curved lines originating from the right side of the 'Classification' bullet point. The top line points to the word 'supervised' and the bottom line points to the word 'unsupervised'.

This covers **EVERYTHING**. (almost)

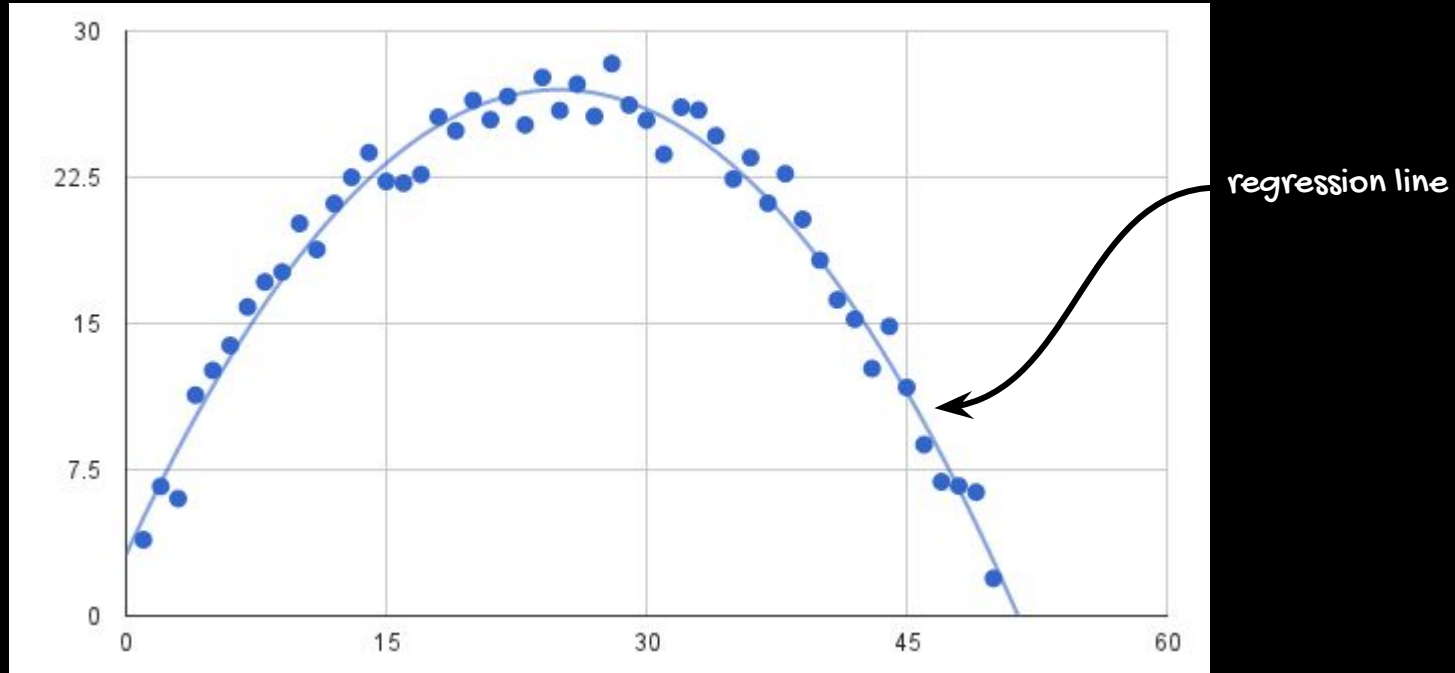
LINEAR REGRESSION



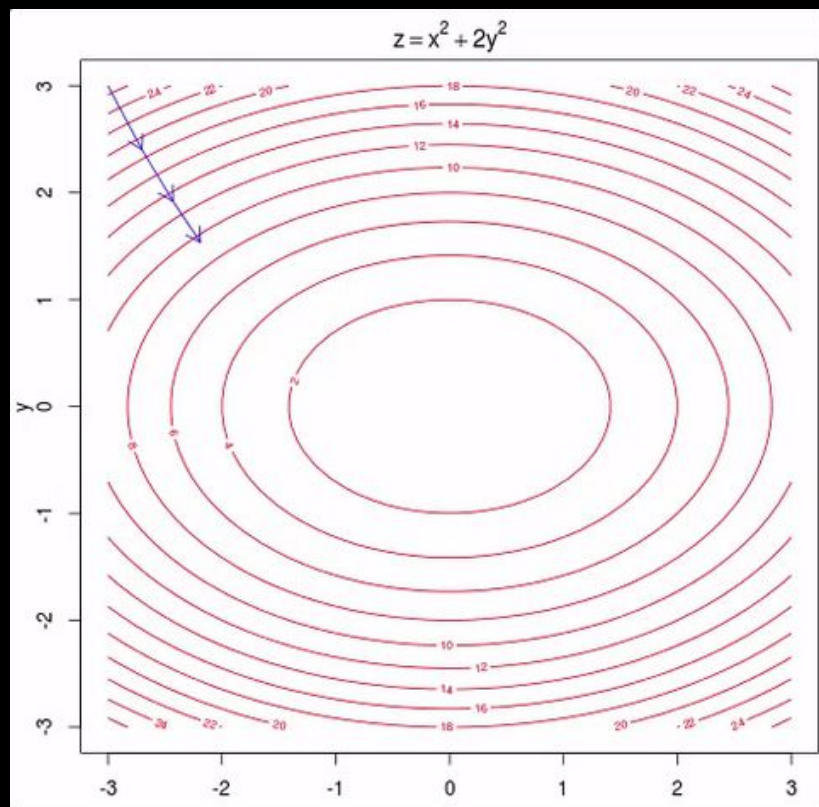
2d linear
regression

regression

POLYNOMIAL REGRESSION

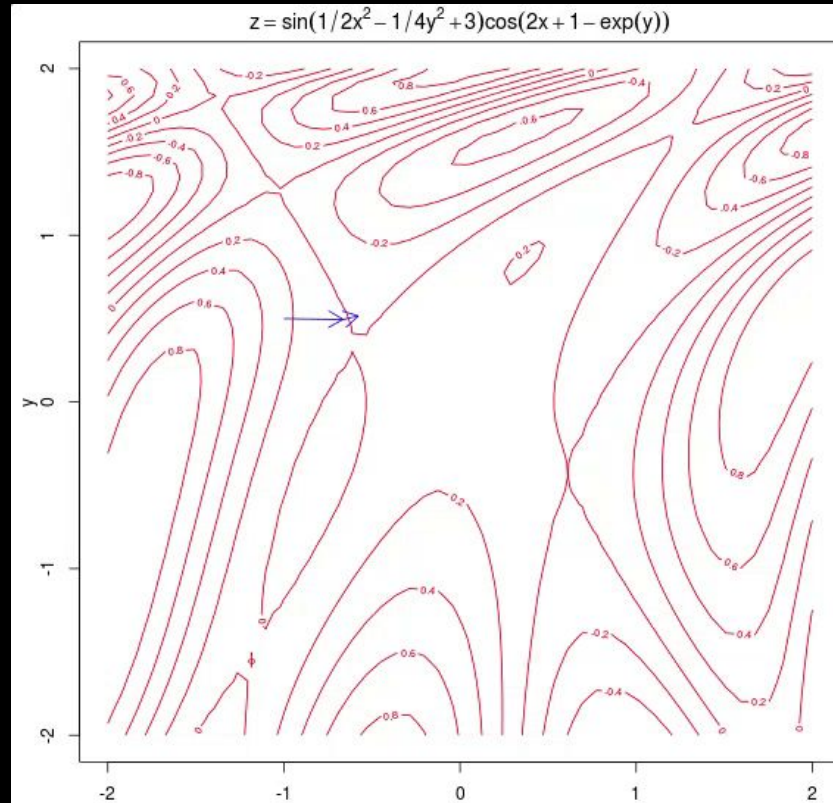


SOLVING



Success

SOLVING

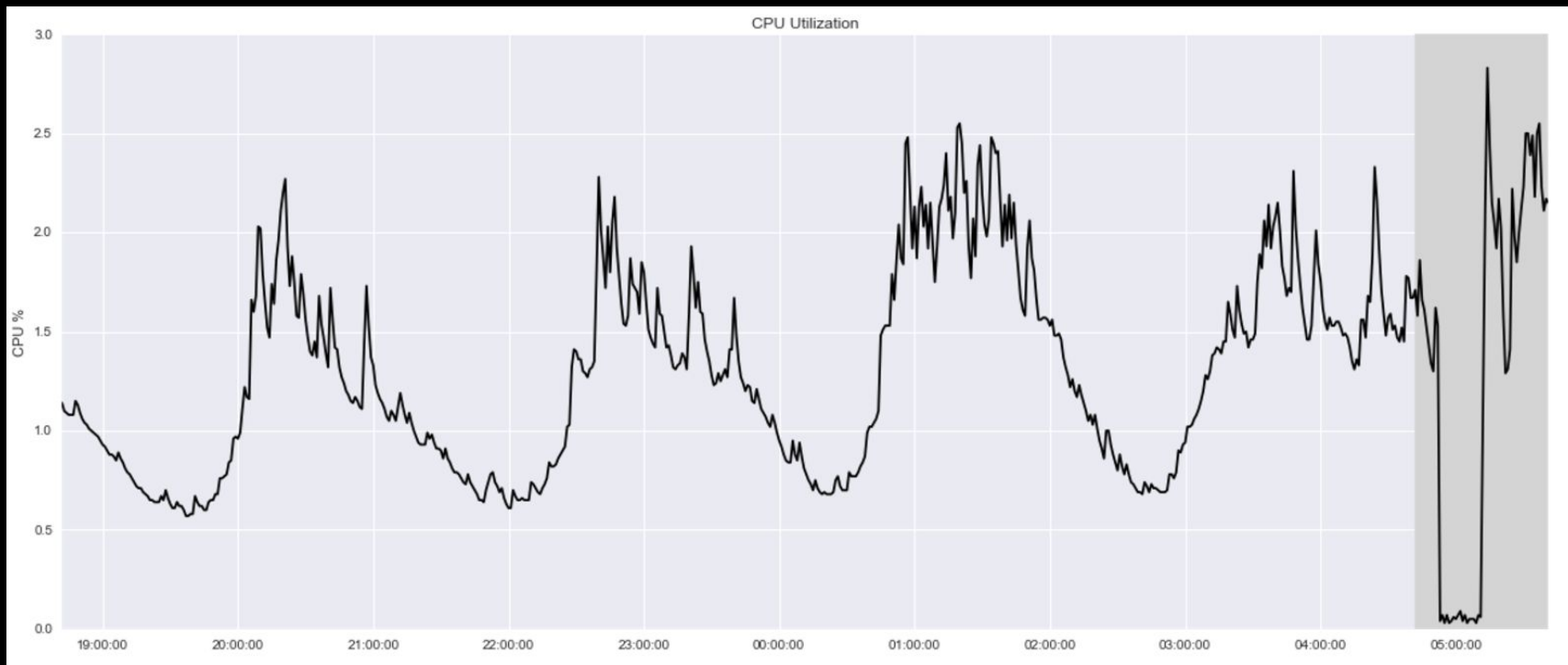


failure

LINEAR/LOGISTIC REGRESSION

- `/home/ml/Desktop/intro/00-linear-regression.ipynb`
- `/home/ml/Desktop/intro/01-logistic-regression.ipynb`

ANOMALY DETECTION



ANOMALY DETECTION

- **Outliers vs. novelties**
 - *novelties*: unobserved pattern in new observations not included in training data
- **Simple statistics/forecasting methods**
 - Exponential smoothing, Holt-Winters algorithm
- **Machine learning methods**
 - Elliptical envelope, density-based, clustering, SVM

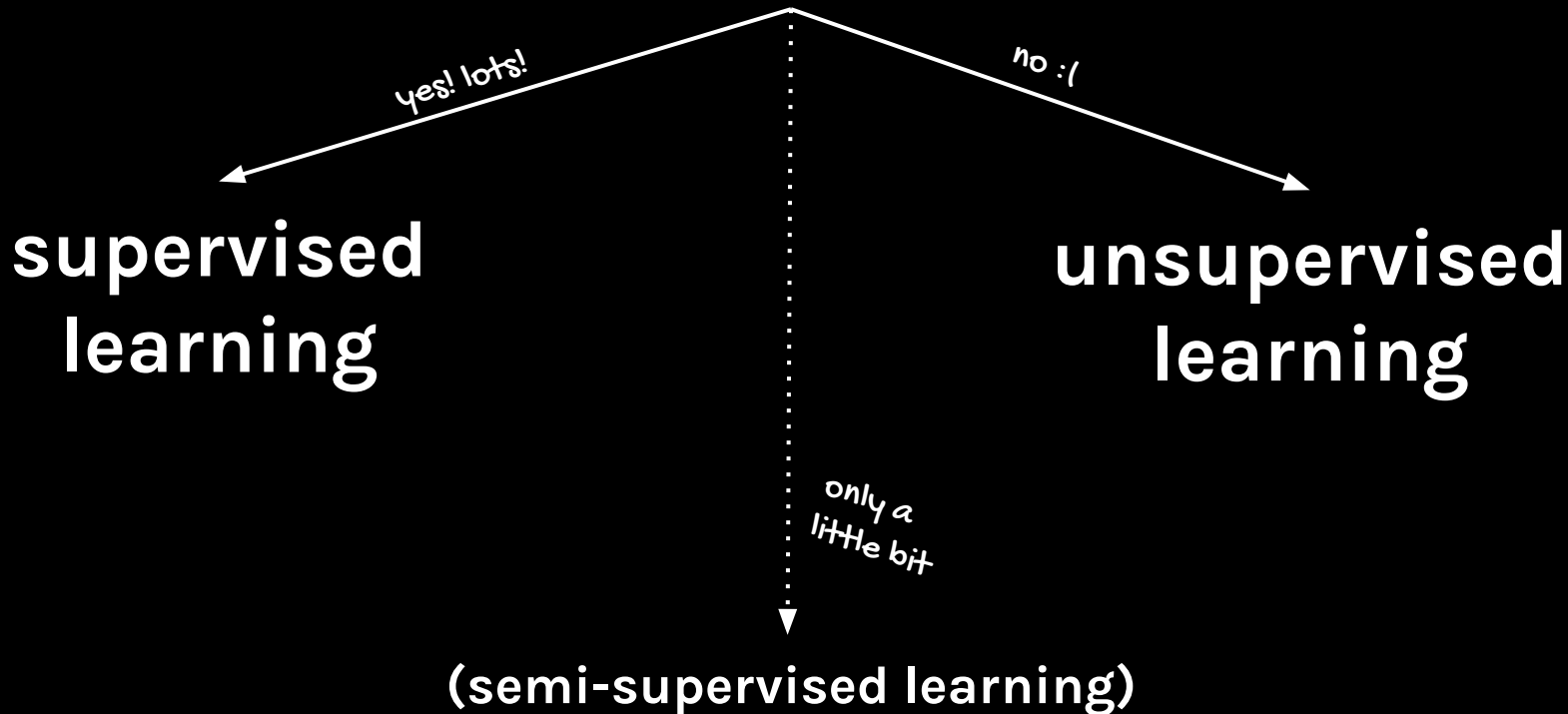
ANOMALY DETECTION

- `/home/ml/Desktop/intro/02-anomaly-detection.ipynb`
- `/home/ml/Desktop/anomaly/anomaly-detection-eg.ipynb`

CLASSIFICATION

labeled data - do you have it?

CLASSIFICATION

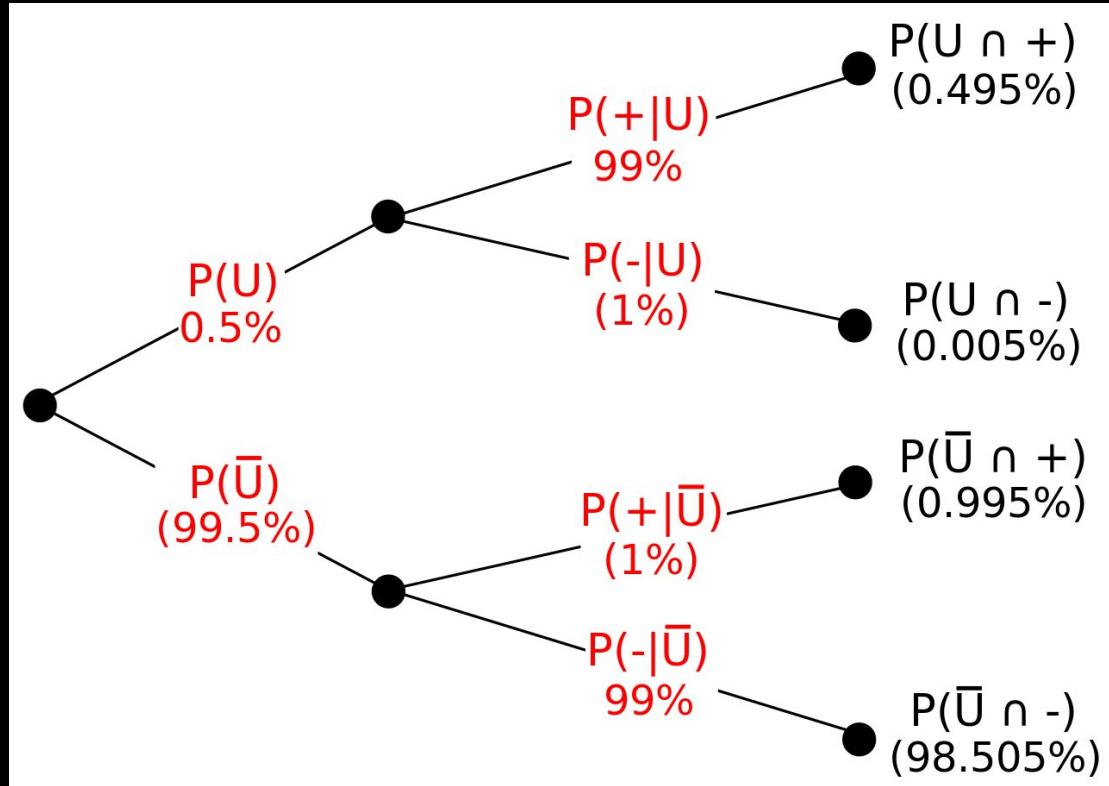


SUPERVISED CLASSIFICATION

- Many different algorithms!
- We will go through five:
 - Naive Bayes
 - K-nearest neighbors
 - Support Vector Machines
 - Decision Trees

BAYES THEOREM

the probability of an event happening is based on prior knowledge of conditions that might be related to the event



NAIVE BAYES CLASSIFIER

- SUPERVISED LEARNING

HANDS ON

CLASSIFYING SPAM

THE DATASET: 2007 TREC Public Spam Corpus

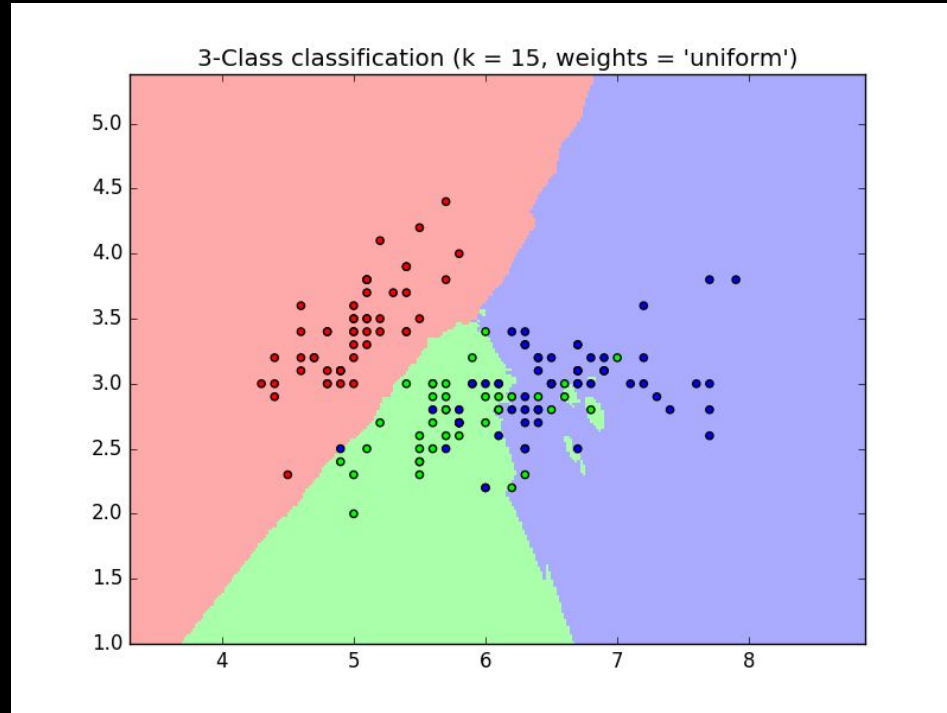
<http://plg.uwaterloo.ca/~gvcormac/treccorpus07/>

MULTICLASS CLASSIFICATION

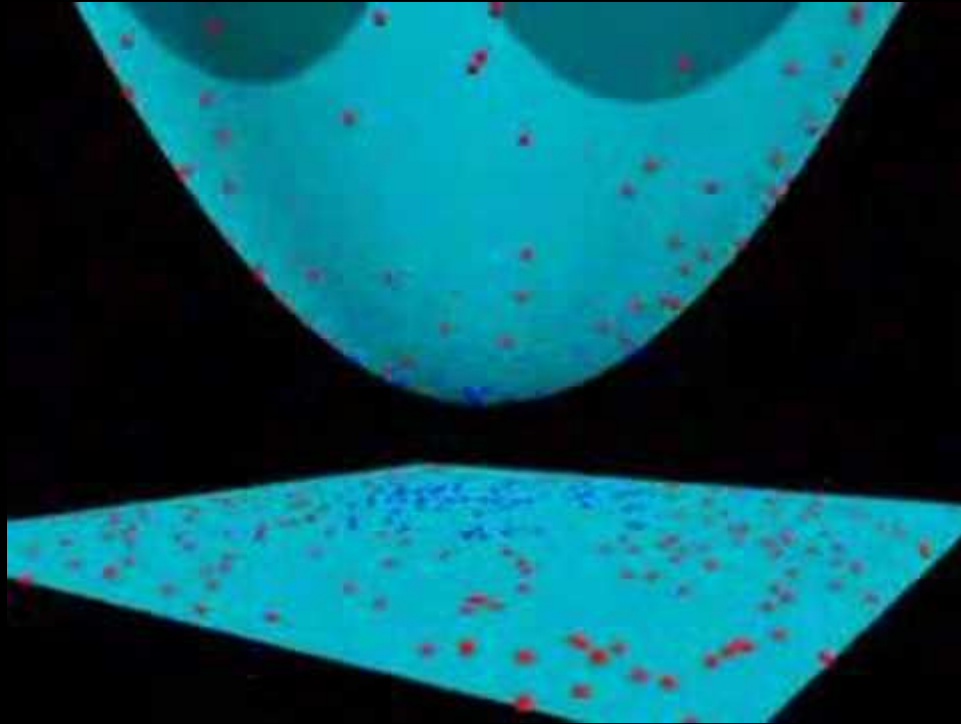
2 ways to do it:

- **1-vs-rest**
 - 1 binary classifier per class
- **1-vs-1**
 - 1 binary classifier per pair of classes
 - $K*(K-1)/2$ classifiers for a K-class problem

K-NEAREST NEIGHBORS CLASSIFIER (kNN)



SUPPORT VECTOR MACHINES (SVM)



- `/home/ml/Desktop/intro/03-svm.ipynb`

DECISION TREE CLASSIFIER

[visualization](#)

UNSUPERVISED CLASSIFICATION

- Mainly refers to clustering
- Four types:
 - Centroid: K-Means
 - Distribution: Gaussian mixture models
 - Density: DBSCAN
 - Connectivity: Hierarchical clustering

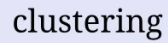
K-MEANS CLUSTERING

- UNSUPERVISED LEARNING

- `/home/ml/Desktop/intro/04-kmeans-pca.ipynb`

SO MANY ALGORITHMS.
HOW TO PICK.?????????

classification



dimensionality
reduction

HANDS ON

XSS DETECTION

- `/home/ml/Desktop/waf`

HANDS ON

CLASSIFYING PACKETS

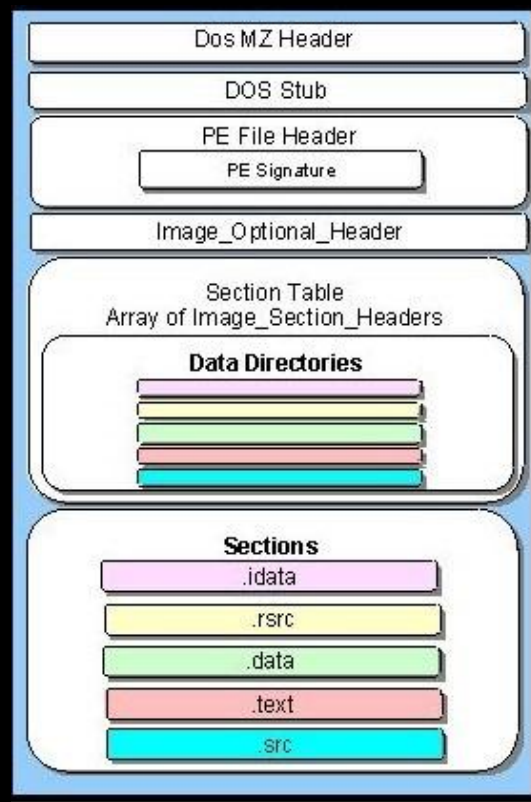
[dataset](#)

- `/home/ml/Desktop/network/kdd-packet-classification.ipynb`

HANDS ON

CLASSIFYING MALWARE (with static PE features)

- `/home/ml/Desktop/malware`



pefile dump

-----Parsing Warnings-----

Suspicious NumberOfRvaAndSizes in the Optional Header. Normal values are never larger than 0x10, the value is: 0xdffffd0de

Error parsing section 2. SizeOfRawData is larger than file.

-----DOS_HEADER-----

[IMAGE_DOS_HEADER]

e_magic: 0x5A4D
e_cblp: 0x50
e_cp: 0x2

-----NT_HEADERS-----

[IMAGE_NT_HEADERS]

Signature: 0x4550

-----FILE_HEADER-----

[IMAGE_FILE_HEADER]

Machine: 0x14C
NumberOfSections: 0x4
TimeDateStamp: 0x851C3163
[INVALID TIME]
PointerToSymbolTable: 0x74726144
NumberOfSymbols: 0x455068
SizeOfOptionalHeader: 0xE0
Characteristics: 0x818F

-----OPTIONAL_HEADER-----

[IMAGE_OPTIONAL_HEADER]

Magic: 0x10B
MajorLinkerVersion: 0x2
MinorLinkerVersion: 0x19
SizeOfCode: 0x200
SizeOfInitializedData: 0x45400
SizeOfUninitializedData: 0x0
AddressOfEntryPoint: 0x2000
BaseOfCode: 0x1000
BaseOfData: 0x2000
ImageBase: 0xDE0000
SectionAlignment: 0x1000
FileAlignment: 0x1000
MajorOperatingSystemVersion: 0x1
MinorOperatingSystemVersion: 0x0

-----PE Sections-----

[IMAGE_SECTION_HEADER]

Name: CODE
Misc: 0x1000
Misc_PhysicalAddress: 0x1000
Misc_VirtualSize: 0x1000
VirtualAddress: 0x1000
SizeOfRawData: 0x1000
PointerToRawData: 0x1000
PointerToRelocations: 0x0
PointerToLinenumbers: 0x0
NumberOfRelocations: 0x0
NumberOfLinenumbers: 0x0
Characteristics: 0xE0000020

Flags: MEM_WRITE, CNT_CODE, MEM_EXECUTE, MEM_READ
Entropy: 0.061089 (Min=0.0, Max=8.0)

[IMAGE_SECTION_HEADER]

Name: DATA
Misc: 0x45000
Misc_PhysicalAddress: 0x45000
Misc_VirtualSize: 0x45000
VirtualAddress: 0x2000
SizeOfRawData: 0x45000

PointerToRawData:

0x2000
PointerToRelocations: 0x0
PointerToLinenumbers: 0x0
NumberOfRelocations: 0x0
NumberOfLinenumbers: 0x0
Characteristics: 0xC0000040
Flags: MEM_WRITE, CNT_INITIALIZED_DATA, MEM_READ
Entropy: 7.980693 (Min=0.0, Max=8.0)

[IMAGE_SECTION_HEADER]

Name: NicolasB
Misc: 0x1000
Misc_PhysicalAddress: 0x1000
Misc_VirtualSize: 0x1000
VirtualAddress: 0x47000
SizeOfRawData: 0xEFEFADFF
PointerToRawData: 0x47000
PointerToRelocations: 0x0
PointerToLinenumbers: 0x0
...

FEATURE VECTOR

Name|md5|Machine|SizeOfOptionalHeader|Characteristics|MajorLinkerVersion|MinorLinkerVersion|SizeOfCode|SizeOfInitializedData|SizeOfUninitializedData|AddressOfEntryPoint|BaseOfCode|BaseOfData|ImageBase|SectionAlignment|FileAlignment|MajorOperatingSystemVersion|MinorOperatingSystemVersion|MajorImageVersion|MinorImageVersion|MajorSubsystemVersion|MinorSubsystemVersion|SizeOfImage|SizeOfHeaders|Checksum|Subsystem|DllCharacteristics|SizeOfStackReserve|SizeOfStackCommit|SizeOfHeapReserve|SizeOfHeapCommit|LoaderFlags|NumberOfRvaAndSizes|SectionsNb|SectionsMeanEntropy|SectionsMinEntropy|SectionsMaxEntropy|SectionsMeanRawsize|SectionsMinRawsize|SectionMaxRawsize|SectionsMeanVirtualsize|SectionsMinVirtualsize|SectionMaxVirtualsize|ImportsNbDLL|ImportsNb|ImportsNbOrdinal|ExportNb|ResourcesNb|ResourcesMeanEntropy|ResourcesMinEntropy|ResourcesMaxEntropy|ResourcesMeanSize|ResourcesMinSize|ResourcesMaxSize|LoadConfigurationSize|VersionInformationSize|**legitimate**

legitimate:

memtest.exe|631ea355665f28d4707448e442bf5b8|332|224|258|9|0|361984|115712|0|6135|4096|372736|4194304|4096|512|0|0|0|0|1|0|1036288|1024|485887|16|1024|1048576|4096|1048576|4096|0|16|8|5.7668065537|3.60742957555|7.22105072892|59712.0|1024|325120|126875.875|896|551848|0|0|0|0|4|3.26282271103|2.56884382364|3.53793936419|8797.0|216|18032|0|16|**1**

malware:

VirusShare_76c2574c22b44f69e3ed519d36bd8dff|76c2574c22b44f69e3ed519d36bd8dff|332|224|258|10|0|28672|445952|16896|14819|4096|32768|4194304|4096|512|5|0|6|0|5|0|3977216|1024|680384|2|34112|1048576|4096|1048576|4096|0|16|6|2.65064184009|0.0|6.49788465186|30634.6666667|0|139264|661773.333333|3978|3362816|8|172|1|0|21|3.42072662405|1.86523352037|7.9688495098|6558.42857143|180|67624|0|0|**0**

THANK YOU

@cchio

cchio@cs.stanford.edu

@antojosep007

antojoseph007@gmail.com

sign up for updates!

`mlsec@cs.stanford.edu`

THANKS

<https://www.amazon.com/Machine-Learning-Security-Protecting-Algorithms/dp/1491979909>

