

Vancouver

INCS 615: Advanced Network and Internet Security

Project: Network Intrusion Detection Using Machine Learning

Instructor: Dr. Zhida Li

Summer 2023 SYLLABUS (INCS 615-VA1)

Email: zli74@nyit.edu

Term Project (group)

Welcome to the group-based project (in groups of up to 3). In this project, we will learn four types of intrusions and use the machine learning model(s) to detect them: **coding (Python)** + **presentation**.

You need to give a presentation on Week 7.2 (July 6). Each group will have 10 minutes (presentation + Q&A)

Term Project carries 20% of your final grade: project code – group (10%) + presentation – group (10%)

Tasks:

1. Download the shared folder from Google Drive:

https://drive.google.com/drive/folders/1Iwd2LqYEJcXfv6mcsCeJ1Sb-C80Q5 z7?usp=sharing

Folder name:

NIDS_using_MachineLearning

Unzip the folder.

Folder content:

- Python code (Jupyter file): INCS615_project_NIDS_ML.ipynb
- NSL-KDD training data (42 columns): KDDTrain+_20Percent_651.csv
- NSL-KDD testing data (42 columns): KDDTest+_651.csv
- Webpage (NSL-KDD) offline: *nsl-kdd_index.html*
- Paper for NSL-KDD: A_detailed_analysis_of_the_KDD_CUP_99_data_set.pdf
- Paper for additional details of NSL-KDD:

A_detailed_analysis_of_the_KDD_CUP_99_data_set.pdf

Content of the CSV files:

Row 1: feature names

Columns 1-41: features

Column 42: labels for regular = 0, DOS = 1, R2L = 2, U2R = 3, Probe = 4.

2. Learn and understand your NSL-KDD data:

Cyber attacks are becoming more sophisticated and, hence, more difficult to detect. Using efficient and effective machine learning techniques to detect network anomalies and intrusions is an important aspect of cyber security.

Machine learning algorithms have been evaluated for robustness, high accuracy, and training time when classifying various datasets collected from communication networks. Reliable testing and validation of anomaly and intrusion detection algorithms depend on the quality of datasets such as traffic collected from deployed networks or experimental testbeds. The most widely used benchmark datasets in the literature are Knowledge Discovery in Databases (KDD) Cup 1999 (KDD'99) and NSL-KDD. KDD'99 intrusion dataset is based on the Defense Advanced Research Projects Agency (DARPA) 1998 dataset.

The NSL-KDD dataset is an improved version of the KDD'99 intrusion dataset. Data were captured from an evaluation testbed and included large numbers of virtual hosts and user automata. The KDD'99 dataset was used in various IDSs. NSL-KDD is a randomly selected subset of KDD'99 after redundant data were removed and is a widely used benchmark for evaluating anomaly detection techniques. NSL-KDD dataset captures TCP, UDP, and Internet Control Message Protocol (ICMP) traffic collected using the tcpdump utility. It contains four types of intrusion attacks: DoS, R2L, U2R, and Probe described in Table 1.

Each network connection is represented by 41 features: 38 numerical and 3 categorical ("protocol_type", "service", and "flag") features. Categorical features will be removed in our experiment.

Table 1: NSL-KDD dataset: Four types of intrusion attacks are listed: DoS, R2L, U2R, and Probe.

Type	Intrusion attacks	
DoS	back, land, neptune, pod, smurf, teardrop, mailbomb,	
	processtable, udpstorm, apache2, worm	
U2R	buffer-overflow, loadmodule, perl, rootkit, sqlattack, xterm, ps	
R2L	fpt-write, guess-passwd, imap, multihop, phf, spy, warezmaster,	
	xlock, xsnoop, snmpguess, snmpgetattack, httptunnel, sendmail,	
	named	
Probe	ipsweep, nmap, portsweep, satan, mscan, saint	

The features with continuous and discrete types are described in Table 2. We consider five-way classification, the targets are regular, DoS, R2L, U2R, and Probe, labeled as 0, 1, 2, 3, and 4, respectively. We employ the KDDTrain+_20Percent_651 dataset for training and KDDTest+_651 dataset for testing.

Table 2: NSL-KDD features: Definitions, types, and descriptions. Each network connection is represented by 41 features: 38 numerical and 3 categorical ("protocol_type", "service", and "flag")

features.

discrete discrete type of the protocol (TCP, UDP) service discrete type of the protocol (TCP, UDP) service discrete type of the protocol (TCP, UDP) service on the destination, (HTTP, telnet) flag discrete continuous continuous no. of data bytes from source to destination no. of data bytes from source to destination to source of otherwise on the same host/port; of otherwise no. of "wrong" fragments no. of wrong" fragments no. of "wrong" fragments no. of wrong "fragments no. of "wrong" fragments no. of "wrong" fra	Feature	Definition	Type	Description
discrete discrete network service on the destination, (HTTP, telhet) flag discrete continuous continuous no. of data bytes from source to destination no. of fuse the same host from/to the same host as the current connection in the past 2 s no. of "noof" roof" ragments no. of "roof" ragments no. of stall pate the pate to suit induse no. of "roof" ragments no. of "roof" ragments no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service	_	duration	continuous	length (seconds) of the connection
4 flag discrete continuous no. of data bytes from source to destination no. of data bytes from source to destination no. of data bytes from destination to source discrete 1 if connection is from/to the same host/port; 0 otherwise no. of "wrong" fragments no. of "hot" indicators no. of failed login attempts 12 logged in discrete 1 if successfully logged in; 0 otherwise no. of "compromised" continuous no. of alied login attempts 13 num_compromised discrete 1 if successfully logged in; 0 otherwise no. of "compromised" conditions no. of shell prompts no. of "sompromised" conditions no. of "compromised" conditions no. of "sompromised" conditions no. of "compromised" conditions no. of "sompromised" conditions no. of shell prompts no. of shell prompts no. of otherwise no. of outbound commands in an ftp session outbound command		protocol_type	discrete	type of the protocol (TCP, UDP)
4 flag 5 src_bytes 6 dst_bytes 7 land 6 myrong_fragment 9 urgent 10 hot 11 num_failed_logins 12 logged_in 13 num_compromised 14 root_shell 15 su_attempted 16 num_root 17 num_falle_creations 18 num_shells 20 num_outbound_cmds 21 is_host_login 22 is_guest_login 23 count 24 srv_count 25-26 serror_rate 27-28 rerror_rate 29 same_srv_rate 27-28 rerror_rate 27-28 rerror_rate 27-28 rerror_rate 30 diff_srv_rate 31 dst_host_srv_serror_rate 32 dst_host_serror_rate 33 dst_host_srv_serror_rate 36 dst_host_srv_serror_rate 36 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-51 discrete continuous continuous continuous and dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-51 discrete continuous	3	service	discrete	network service on the destination,
5 src_bytes continuous 6 dst_bytes continuous 7 land discrete 1 if connection is from/to the same host/port; 0 otherwise 10 hot continuous 11 num_failed_logins continuous 12 logged_in discrete 1 if successfully logged in; 0 otherwise 13 num_compromised continuous 14 root_shell discrete 1 if successfully logged in; 0 otherwise 15 su_attempted discrete 1 if successfully logged in; 0 otherwise 16 num_root continuous 17 num_falle_creations continuous 18 num_shells continuous 19 num_access_files continuous 20 num_outbound_crnds continuous 21 is_host_login discrete 1 if the login is a "guest"login; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise 23 count continuous continuous as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the p				(HTTP, telnet)
6 dst_bytes 7 land discrete 8 wrong_fragment continuous 9 urgent continuous 10 hot continuous 11 num_failed_logins continuous 12 logged_in discrete 13 num_compromised continuous 14 root_shell discrete 15 su_attempted discrete 16 num_root continuous 17 num_file_creations continuous 18 num_access files continuous 19 num_access files continuous 20 num_outbound_cmds 21 is_host_login discrete 23 count continuous 24 srv_count continuous 25-26 serror_rate and srv_serror_rate 27-28 rerror_rate and srv_serror_rate 27-28 rerror_rate and srv_serror_rate 27-28 rerror_rate and srv_serror_rate 30 diff_srv_rate 31 dst_host_srv_count 32 dst_host_same_srv_rate 35 dst_host_same_srv_rate 36 dst_host_same_srv_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_srv_serror_rate 40-41 dst	4	flag	discrete	normal or error status of the connection
Second	5	src_bytes	continuous	no. of data bytes from source to destination
8 wrong_fragment continuous no. of "wrong" fragments no. of "wrong inclinate phont in the pack 2 send in the pac	6	dst_bytes	continuous	no. of data bytes from destination to source
9 urgent continuous no. of urgent packets no. of "hot" indicators no. of file login attempts 11 num_failed_logins continuous no. of filed login attempts 12 logged_in discrete 1 if successfully logged in; 0 otherwise no. of "compromised" conditions 14 root_shell discrete 1 if "su root" command attempted; 0 otherwise 15 su_attempted discrete 1 if "su root" command attempted; 0 otherwise 16 num_root continuous no. of shell is obtained; 0 otherwise 17 num_file_creations continuous no. of shell prompts no. of shell prompts no. of operations on access control files continuous no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; 0 otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service and srv_serror_rate 29 same_srv_rate continuous and srv_serror_rate and srv_serror_rate 29 same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of conne	7	land	discrete	
10 hot num_failed_logins continuous no. of "hot" indicators no. of failed login attempts 12 logged_in discrete 1 if successfully logged in; 0 otherwise no. of failed login attempts 14 root_shell discrete 1 if successfully logged in; 0 otherwise no. of "compromised" conditions 1 if root_shell is obtained; 0 otherwise 1 if "su root" normand attempted; 0 otherwise no. of "root" accesses number of file creation operations no. of shell prompts no. of shell prompts no. of otherwise no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; 0 otherwise no. of connections to the same service and srv_serror_rate 2 same_srv_rate 2 same_srv_rate 2 dst_host_srv_count 2 continuous 2 dst_host_srv_rate 3 dst_host_same_srv_rate 3 dst_host_srv_rate 3 dst_host_same_srv_rate 3 dst_host	8	wrong_fragment	continuous	no. of "wrong" fragments
11 num_failed_logins 12 logged_in 13 num_compromised 14 root_shell 15 su_attempted 16 num_root 17 num_file_creations 18 num_access_files 19 num_access_files 20 num_outbound_cmds 21 is_host_login 22 is_guest_login 23 count 24 srv_count 25-26 serror_rate 27-28 rerror_rate 29 same_srv_rate 29 same_srv_rate 21 sy_diff_host_rate 29 same_srv_rate 30 diff_srv_rate 31 sv_diff_host_rate 32 dst_host_soun_srv_rate 33 dst_host_srv_count 34 dst_host_srv_cuilf_host_rate 35 dst_host_same_srv_port_rate 36 dst_host_same_srv_perror_rate 37 dst_host_srv_eerror_rate 38-39 ddt_host_srv_error_rate 40-41 dst_host_rerror_rate 40-41	9	urgent	continuous	no. of urgent packets
12 logged_in num_compromised continuous no. of "compromised" conditions 14 root_shell discrete 1 if root_shell is obtained; 0 otherwise 1 if root_shell is obtained; 0 otherwise 1 if "out_root" command attempted; 0 otherwise 2 otherwise 2 otherwise 2 num_file_creations 2 continuous 2 num_file_creations 2 continuous 2 num_outbound_cmds 2 continuous 2 num_outbound_cmds 2 is_host_login 2 is_guest_login 2 is_guest_login 3 count 4 continuous 2 is_guest_login 4 continuous 2 is_guest_login 4 continuous 2 is_guest_login 5 count 6 continuous 2 is_guest_login 6 count 6 continuous 7 continuous 8 continuous 8 count 8 count 8 count 9 continuous 9 continuous 9 continuous 9 continuous 9 continuous 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 if the login is a "guest"login; 0 otherwise 1 is the current co	10	hot	continuous	no. of "hot" indicators
num_compromised discrete 1 if root shell is obtained; 0 otherwise 1 if root sh	11	num_failed_logins	continuous	no. of failed login attempts
14 root_shell discrete discrete 1 if root shell is obtained; 0 otherwise 1 if "su root" command attempted; 0 otherwise 1 otherwise 2 is_guest_login discrete 2 is_guest_login discrete 2 is_guest_login discrete 2 if the login belongs to the "hot" list; 0 otherwise 2 otherwise 1 if the login is a "guest"login; 0 otherwise 2 otherwise 1 if the login is a "guest"login; 0 otherwise 2 otherwise 2 otherwise 1 if the login is a "guest"login; 0 otherwise 2	12	logged_in	discrete	1 if successfully logged in; 0 otherwise
15 su_attempted discrete 0 otherwise 16 num_root continuous no. of "root" accesses 17 num_file_creations continuous no. of shell prompts 18 num_shells continuous no. of shell prompts 19 num_access_files continuous no. of operations on access control files 20 num_outbound_cmds continuous no. of outbound commands in an ftp session 21 is_host_login discrete 1 if the login belongs to the "hot" list; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise 23 count continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to different hosts no. of connections to the same source port no. of connections that have "SYN" errors no. of conn	13	$num_compromised$	continuous	no. of "compromised" conditions
16 num_root continuous number of file creation operations on of shell prompts no. of operations on access control files no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; of otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections to the same service no. of connections to different services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same se	14	$root_shell$	discrete	1 if root shell is obtained; 0 otherwise
16 num_root continuous no. of "root" accesses number of file creation operations no. of shell prompts no. of operations no. of shell prompts no. of operations no. of shell prompts no. of operations no. of opera	15	$su_attempted$	discrete	1 if "su root" command attempted;
num_file_creations num_shells num_access_files num_outbound_cmds is_host_login continuous continuous discrete is_guest_login continuous continuous continuous discrete is_guest_login continuous continuous continuous discrete is_guest_login continuous continuous continuous continuous discrete if the login belongs to the "hot" list; 0 otherwise 1 if the login is a "guest"login; 0 otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same services no. of connections to the same services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to				0 otherwise
num_shells continuous no. of shell prompts num_access_files continuous no. of operations on access control files num_outbound_cmds continuous no. of outbound commands in an ftp session discrete 1 if the login belongs to the "hot" list; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same source port no. of connections to the same source port no. of connections that have "SYN" errors no. of connections that have "S	16	num_root	continuous	no. of "root" accesses
num_access_files num_outbound_cmds continuous no. of operations on access control files no. of outbound commands in an ftp session 1 if the login belongs to the "hot" list; 0 otherwise 22 is_guest_login discrete 1 if the login is a "guest"login; 0 otherwise 23 count continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate 27-28 rerror_rate and srv_rerror_rate 29 same_srv_rate continuous 30 diff_srv_rate 31 srv_diff_host_rate continuous 32 dst_host_count continuous 33 dst_host_srv_count continuous continuous continuous no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of co	17	$num_file_creations$	continuous	number of file creation operations
num_outbound_cmds is_host_login discrete 1 if the login belongs to the "hot" list; 0 otherwise 22 is_guest_login discrete 1 if the login belongs to the "hot" list; 0 otherwise 23 count continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate 27-28 rerror_rate and srv_rerror_rate 29 same_srv_rate continuous 30 diff_srv_rate 31 srv_diff_host_rate 32 dst_host_count continuous 33 dst_host_same_srv_rate 34 dst_host_same_srv_rate 35 dst_host_diff_srv_rate 36 dst_host_same_src_port_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_srv_gerror_rate 40-41 dst_host_srv_serror_rate continuous no. of connections to the same source port no. of connections to the same source port no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the pa	18	num_shells	continuous	no. of shell prompts
is_host_login discrete lif the login belongs to the "hot" list; o otherwise lif the login is a "guest"login; 0 otherwise lif the login is a "guest"login; 0 otherwise no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate continuous no. of connections that have "REJ" errors no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of con	19	num_access_files	continuous	no. of operations on access control files
is_guest_login discrete continuous no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections that have "REJ" errors no. of connections to the same service no. of connections to the same service no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service no. of connections to the same service no. of connections to the same service no. of connections to the same source port no. of connections to different hosts no. of connections to different hosts no. of connections to different hosts no. of connections to the same source port no. of connections to different hosts no. of connections to the same source port no. of connections to the same source no. of	20	$num_outbound_cmds$	continuous	no. of outbound commands in an ftp session
22 is_guest_login discrete continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate 27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection to the same service as the current connection to the same service as the current connections to different services no. of connections to different services no. of connections to the same source port no. of connections to the same source port no. of connections to the same source port no. of connections to the same service no. of connect	21	is_host_login	discrete	1 if the login belongs to the "hot" list;
count continuous no. of connections to the same host as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors no. of connections that have "REJ" errors no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same source port no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections t				0 otherwise
as the current connection in the past 2 s 24 srv_count continuous 15 serror_rate 25-26 serror_rate 27-28 rerror_rate and srv_rerror_rate 27-28 rerror_rate and srv_rerror_rate 29 same_srv_rate 30 diff_srv_rate 31 srv_diff_host_rate 32 dst_host_count 33 dst_host_srv_count 34 dst_host_srv_count 35 dst_host_same_srv_rate 36 dst_host_same_src_port_rate 37 dst_host_same_src_port_rate 38-39 dst_host_srv_diff_host_rate 39 continuous 30 dst_host_srv_rate 30 diff_srv_rate 31 srv_diff_srv_rate 32 dst_host_srv_count 33 dst_host_srv_count 34 dst_host_same_srv_rate 35 dst_host_same_src_port_rate 36 dst_host_same_src_port_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_srv_diff_host_rate 38-39 dst_host_srv_serror_rate 40-41 dst_host_srv_serror_rate 40-41 dst_host_srrerror_rate 40-41 dst_host_srrerror_rate 40-41 dst_host_srrerror_rate 40-41 dst_host_srrerror_rate 40-41 continuous 40-41 continuous	22	is_guest_login	discrete	1 if the login is a "guest" login; 0 otherwise
24 srv_count continuous no. of connections to the same service as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate continuous no. of connections that have "SYN" errors and srv_serror_rate continuous no. of connections that have "REJ" errors no. of connections to the same service no. of connections to the same service no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service no. of connections to different hosts no. of connections to the same source port dst_host_srv_diff_host_rate continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "REJ" errors	23	count	continuous	no. of connections to the same host
as the current connection in the past 2 s no. of connections that have "SYN" errors and srv_serror_rate 27-28 rerror_rate and srv_rerror_rate 29 same_srv_rate continuous 30 diff_srv_rate continuous 31 srv_diff_host_rate continuous 32 dst_host_count continuous 33 dst_host_srv_count 34 dst_host_same_srv_rate 35 dst_host_diff_srv_rate 36 dst_host_same_src_port_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_srv_serror_rate 39 continuous 40-41 dst_host_rerror_rate 40-41 dst_host_rerror_rate 40-41 dst_host_reror_rate 40-41 dst_host_r				as the current connection in the past 2 s
25-26 serror_rate continuous no. of connections that have "SYN" errors and srv_serror_rate 27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors 29 same_srv_rate continuous no. of connections to the same service 30 diff_srv_rate continuous no. of connections to different services 31 srv_diff_host_rate continuous no. of connections to different hosts 32 dst_host_count continuous no. of connections to different hosts 33 dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s 34 dst_host_same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s 35 dst_host_diff_srv_rate continuous no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to different services no. of connections to the same source port no. of connections to the same source port continuous no. of connections to the same source port no. of connections to different hosts 38-39 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_srv_serror_rate continuous no. of connections to the same source port no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	24	srv_count	continuous	
and srv_serror_rate 27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors 29 same_srv_rate continuous no. of connections to the same service 30 diff_srv_rate continuous no. of connections to different services 31 srv_diff_host_rate continuous no. of connections to different hosts 32 dst_host_count continuous no. of connections to the same service 33 dst_host_srv_count continuous no. of connections to the same service 34 dst_host_same_srv_rate continuous no. of connections to the same service 35 dst_host_diff_srv_rate continuous no. of connections to the same service 36 dst_host_same_src_port_rate continuous no. of connections to different services 37 dst_host_srv_diff_host_rate continuous no. of connections to the same source port 38-39 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_srv_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors				
27-28 rerror_rate and srv_rerror_rate continuous no. of connections that have "REJ" errors continuous no. of connections to the same service no. of connections to different services no. of connections to different services no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different services no. of connections to the same source port continuous no. of connections to the same source port no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	25-26	serror_rate	continuous	no. of connections that have "SYN" errors
29 same_srv_rate continuous no. of connections to the same service 30 diff_srv_rate continuous no. of connections to different services 31 srv_diff_host_rate continuous no. of connections to different hosts 32 dst_host_count continuous no. of connections to the same service 33 dst_host_srv_count continuous no. of connections to the same service 34 dst_host_same_srv_rate continuous no. of connections to the same service 35 dst_host_diff_srv_rate continuous no. of connections to the same service 36 dst_host_same_src_port_rate continuous no. of connections to different services 37 dst_host_srv_diff_host_rate continuous no. of connections to the same source port continuous no. of connections to different hosts 38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors		and srv_serror_rate		
30 diff_srv_rate continuous no. of connections to different services 31 srv_diff_host_rate continuous no. of connections to different hosts 32 dst_host_count continuous no. of connections to the same service as the current connection in the past 2 s 33 dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s 34 dst_host_same_srv_rate continuous no. of connections to the same service 35 dst_host_diff_srv_rate continuous no. of connections to different services 36 dst_host_same_src_port_rate continuous no. of connections to the same source port continuous no. of connections to different hosts 38-39 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_srv_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors and dst_host_srv_serror_rate continuous no. of connections that have "REJ" errors	27-28		continuous	
31 srv_diff_host_rate continuous no. of connections to different hosts no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different services no. of connections to the same source port continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	29		continuous	no. of connections to the same service
dst_host_count continuous no. of connections to the same service as the current connection in the past 2 s dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s dst_host_same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s dst_host_same_srv_rate continuous no. of connections to the same service no. of connections to different services dst_host_same_src_port_rate continuous no. of connections to the same source port continuous no. of connections to different hosts dst_host_srv_diff_host_rate continuous no. of connections that have "SYN" errors and dst_host_srv_serror_rate no. of connections that have "SYN" errors dst_host_rerror_rate continuous no. of connections that have "REJ" errors	30		continuous	no. of connections to different services
as the current connection in the past 2 s 33 dst_host_srv_count 34 dst_host_same_srv_rate 35 dst_host_diff_srv_rate 36 dst_host_same_src_port_rate 37 dst_host_srv_diff_host_rate 38-39 dst_host_serror_rate 38-39 dst_host_srv_serror_rate 38-39 dst_host_srv_serror_rate 39-40-41 dst_host_rerror_rate 40-41 dst_host_rerror_rate 40-41 dst_host_rerror_rate 38 the current connection in the past 2 s no. of connections to the same service no. of connections to different services no. of connections to different hosts continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	31	$srv_diff_host_rate$	continuous	no. of connections to different hosts
dst_host_srv_count continuous no. of connections to the same service as the current connection in the past 2 s dst_host_same_srv_rate continuous no. of connections to the same service as the current connection in the past 2 s no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to different services continuous no. of connections to the same service continuous no. of connections to different services no. of connections to the same source port continuous no. of connections to different hosts continuous no. of connections to the same service continuous no. of connections to the same service no. of connections to the same service continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	32	dst_host_count	continuous	no. of connections to the same service
as the current connection in the past 2 s 34				as the current connection in the past 2 s
dst_host_same_srv_rate continuous no. of connections to the same service dst_host_diff_srv_rate continuous no. of connections to different services dst_host_same_src_port_rate continuous no. of connections to different services continuous no. of connections to the same source port continuous no. of connections to different hosts dst_host_srv_diff_host_rate continuous no. of connections to different hosts continuous no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to the same service no. of connections to the same service continuous no. of connections to the same service no. of connections to the same service continuous no. of connections to different hosts no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "REJ" errors	33	$dst_host_srv_count$	continuous	no. of connections to the same service
dst_host_diff_srv_rate continuous no. of connections to different services dst_host_same_src_port_rate continuous no. of connections to different services continuous no. of connections to different services no. of connections to different services no. of connections that have "SYN" errors				•
36 dst_host_same_src_port_rate continuous no. of connections to the same source port 37 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors and dst_host_srv_serror_rate no. of connections that have "SYN" errors 40-41 dst_host_rerror_rate continuous no. of connections that have "REJ" errors				
37 dst_host_srv_diff_host_rate continuous no. of connections to different hosts 38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors and dst_host_srv_serror_rate no. of connections that have "SYN" errors 40-41 dst_host_rerror_rate continuous no. of connections that have "REJ" errors			continuous	
38-39 dst_host_serror_rate continuous no. of connections that have "SYN" errors no. of connections that have "SYN" errors no. of connections that have "SYN" errors dst_host_rerror_rate continuous no. of connections that have "REJ" errors				_
and dst_host_srv_serror_rate no. of connections that have "SYN" errors dst_host_rerror_rate continuous no. of connections that have "REJ" errors				
40-41 dst_host_rerror_rate continuous no. of connections that have "REJ" errors	38-39		continuous	
and dst_host_srv_rerror_rate	40-41		continuous	no. of connections that have "REJ" errors
		and dst_host_srv_rerror_rate		

References:

[1] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Ottawa, ON, Canada, July 2009, pp. 1–6.

[2] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory," *ACM Trans. Inform. Syst. Secur.*, vol. 3, no. 4, pp. 262–294, Nov. 2000.

3. Go back to Google Drive:

Create your own copy of the folder:

NIDS_using_MachineLearning_teamNo

* Note: This is very important so that you do not alter the original code.

While in your own folder on Google Drive, upload your data, run (double click) on: *INCS615 project NIDS ML.ipynb*

Note:

We assume that you do not already have the Colab web application. To use Colab, select "Open with", search for Application named Colaboratory, and install it. Finally, connect to the Application.

For advanced users only:

In case you wish to run the exercise locally, you need to install Jupyter development environment.

Instructions are posted at:

https://jupyter-notebook.readthedocs.io/en/stable/

To install Jupyter, you will also need the "pip" package management system (installer) for Python:

python get-pip.py

Instruction is available at:

https://jupyter.org/install

4. You are now ready to follow the steps:

INCS615_project_NIDS_ML.ipynb

Machine learning libraries may be used:

- https://scikit-learn.org/stable/index.html
- https://pandas.pydata.org/
- https://pytorch.org/
- https://www.tensorflow.org/

Resources

Journals

- IEEE Communications Surveys & Tutorials
- IEEE Network The Magazine of Global Internetworking
- IEEE Communications Magazine
- ACM Computer Communication Review
- IEEE Journal on Selected Areas in Communications
- IEEE Transactions on Cybernetics
- IEEE Transactions on Systems, Man, and Cybernetics
- <u>IEEE/ACM Transactions on Networking</u>

Note:

Papers from ACM: https://libguides.nyit.edu/az.php?s=16453&a=a&p=1, select "ACM Digital Library", then log in.

Papers from IEEE Explore: https://libguides.nyit.edu/az.php?s=16453&a=i&p=1, select "IEEE Xplore", then log in.

Citation style

Please follow the IEEE citation style when writing references:

- IEEE Editorial Style Manual: https://journals.ieeeauthorcenter.ieee.org/create-your-ieee-article/createthe-text-of-yourarticle/ieee-editorial-style-manual/
- IEEE Reference Guide: http://journals.ieeeauthorcenter.ieee.org/wp-content/uploads/sites/7/IEEE_Reference_Guide.pdf

How to Present Your Project

10 minutes of presentation + 1 minute of Q&A

Make sure all team members are present and that everyone gets properly introduced.

First slide outline:

INCS 615: Advanced Network and Internet Security
Summer 2023
Term Project Presentation
PROJECT TITLE

YOUR NAME(s) YOUR NYIT STUDENT IDS YOUR E-MAIL ADDRESS(es) YOUR TEAM #

Consecutive slides:

1. INTRODUCTION TO THE PROJECT

Introduce the project. Include motivation and overview. Describe the project idea, its scope, and what you are trying to accomplish. State the most important aspect of the project. Present an overall, high-level description of your project.

2. OVERVIEW OF RELATED WORK

Include a short overview and description of related work and state-of-the-art that you have cited in references. The related work can include the application of IDS and the use of machine learning for classifying NSL-KDD data.

3. PROBLEM DESCRIPTION

Provide technical details of the problem that you plan to address/discuss.

4. IMPLEMENTATION

Include data analysis, machine learning algorithm (s), results, and analysis (even if not completed). Include descriptions of the overall design, use flowcharts for sections of the design as needed, and high-level architecture (if appropriate).

5. DISCUSSION

Describe what made it a non-trivial task and what the difficulties were. Suggest alternative approaches to the solution. Suggest improvements and future work. Describe briefly what you have learned from this project.

6. REFERENCES

List the references used and give credits to people whose work you used.

7. CONTRIBUTIONS

List the contributions of the individual team members.

Grading Scheme

CLASS PRESENTATION (total 100 points)

- 1. Introduction to the project: motivation and overview (5 points)
- 2. Overview (20 points)
- 3. Problem description: technical details (20 points)
- 4. Implementation: (even if not completed) (50 points)
- 5. Organization and time management (5 points)

Please Submit:

• **Code** (py or *ipynb*) and **Presentation slides** (PowerPoint and PDF files) of your term project.

Submit the file(s) for your project submission to the Canvas site.

- Include the cover page.
- Note:

More credit will be given to completed projects (even if they are less difficult) than to the ambitious unfinished work.

In the case of team work, we will make every attempt to evaluate the individual performance of each team member.

Good luck!