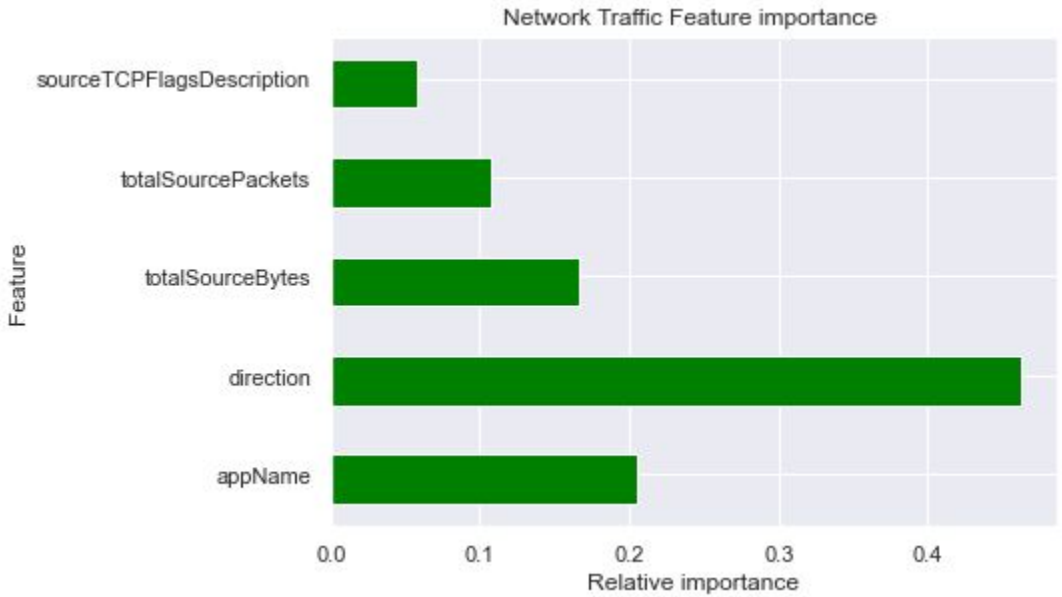
UMDIC2022 - Cybersecurity

Ben Nordmann and Jay Siliphet

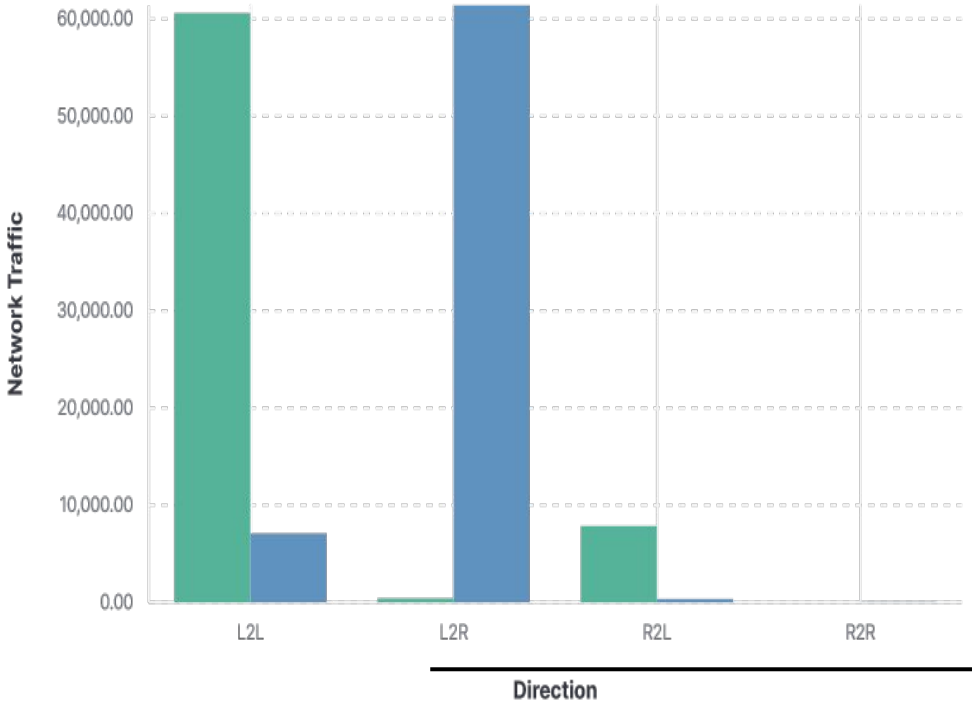
The Model

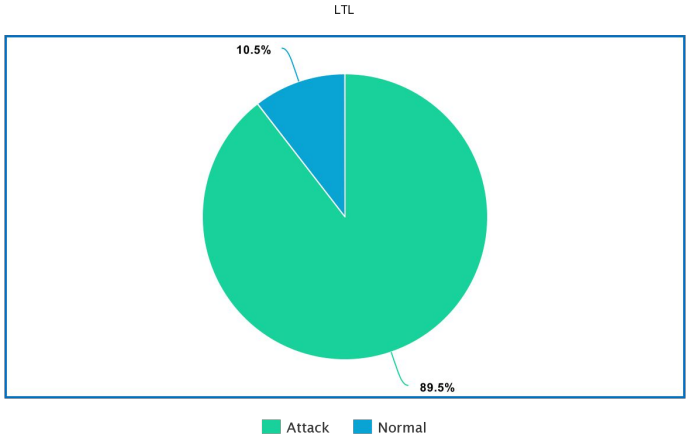
- Random Forest Classification Model
- Accuracy rate of approximately 99.5%
- Multiple iterations to narrow feature selection
- Trained on iscxIDS2012 data set

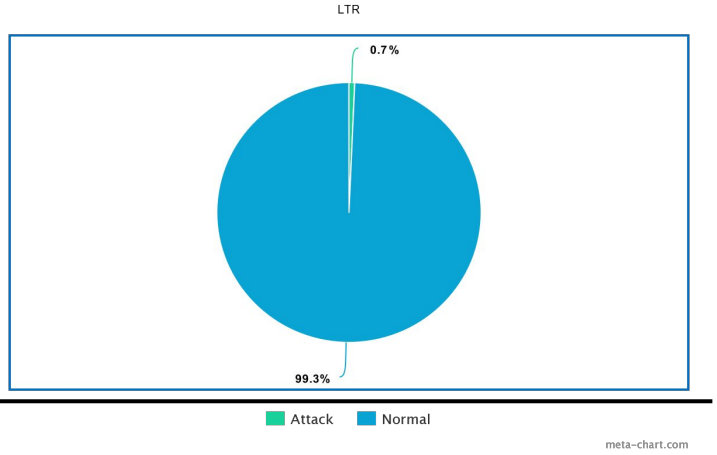
Feature Importance



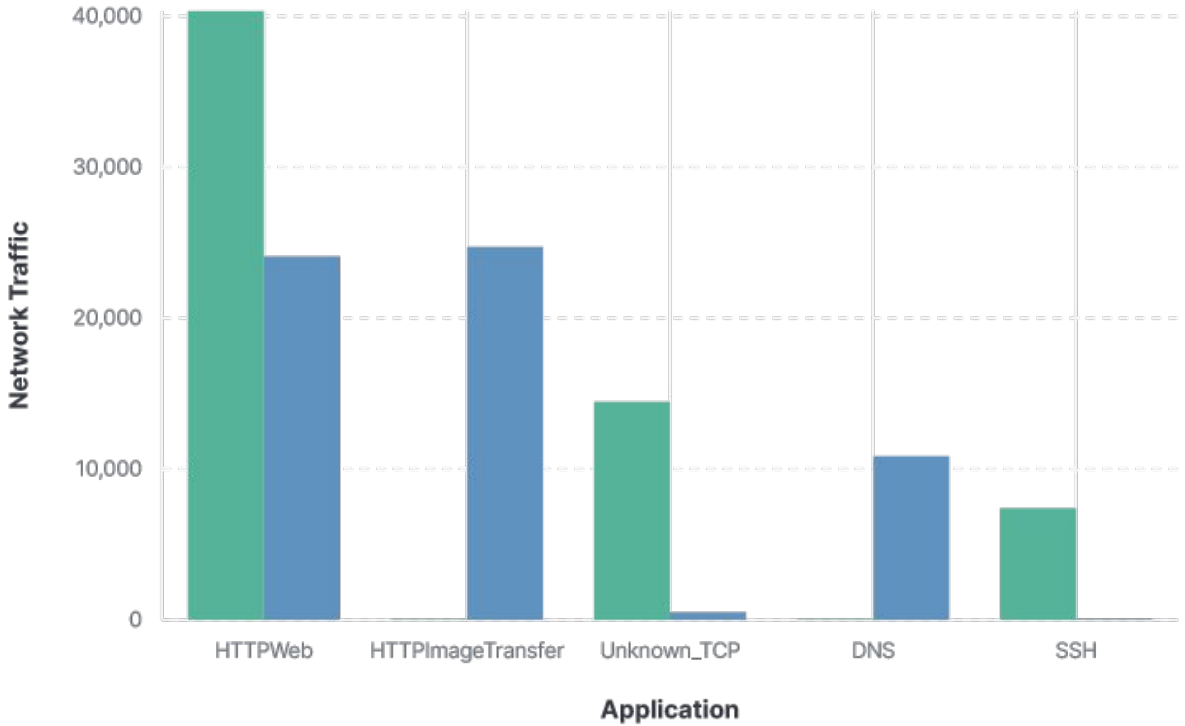
Direction


Network Traffic
60,000.00
50,000.00
40,000.00
30,000.00
20,000.00
10,000.00
0.00
L2L
L2R
R2L
R2R
Direction


LTL
10.5%
89.5%
Attack
Normal
meta-chart.com


LTR
0.7%
99.3%
Attack
Normal
meta-chart.com

appName


40,000
30,000
20,000
10,000
0
Network Traffic
HTTPWeb
HTTPImageTransfer
Unknown_TCP
DNS
SSH
Application

Cyber Kill Chain

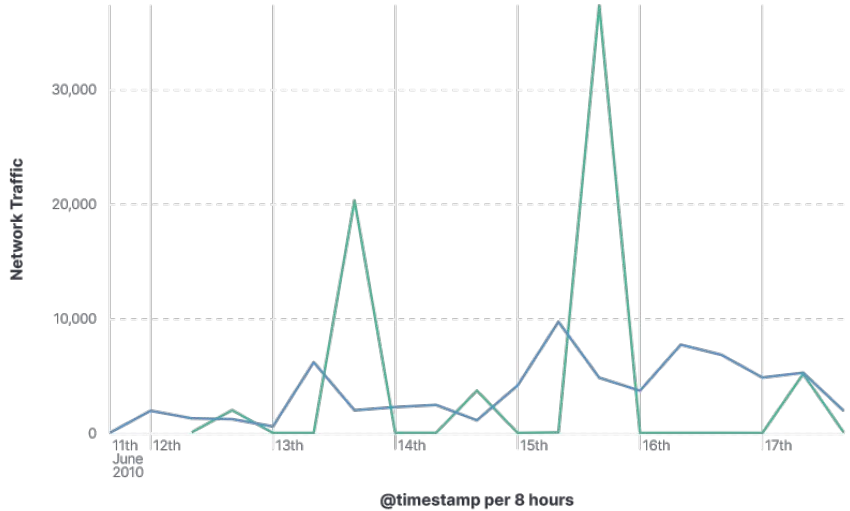
- Dataset does not appear to show port scans
- Weaponization occurs outside the network
- The attacker escalates to command and control almost immediately

Initial Attack

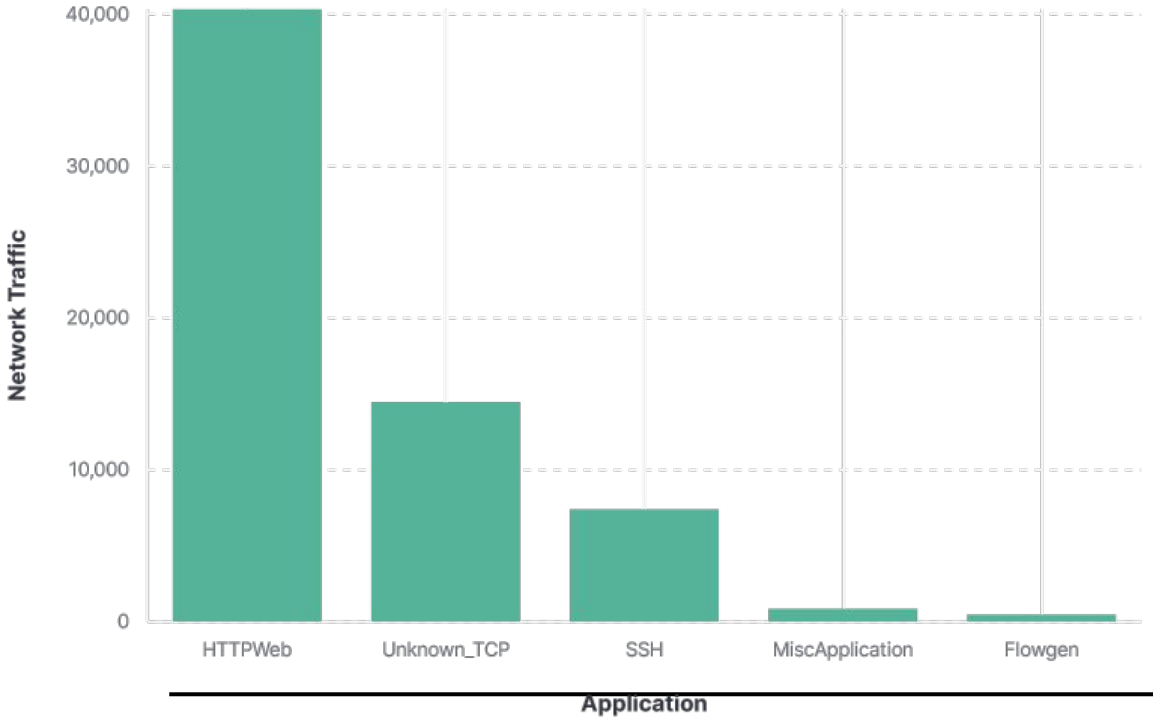
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	34657	F,S,R,A	2010-06-1	2010-06-1	327	4	346	5
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	45410	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	45991	F,S,P,A	2010-06-1	2010-06-1	2721	15	1384	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	46449	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	46979	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	47466	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	48042	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	48508	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	49108	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	49538	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	50099	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	50486	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	50906	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	51515	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	52038	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	52638	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	53000	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	53591	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	54012	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	54522	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	54855	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	55282	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	55765	F,S,P,A	2010-06-1	2010-06-1	2721	15	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	56245	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	56688	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12
Attack	SSH	192.168.5.	-	-	22	F,S,P,A	R2L	tcp_ip	67.23.167	TestbedSa	-	-	57068	F,S,P,A	2010-06-1	2010-06-1	2651	14	1368	12

C2 and Actions on Objectives

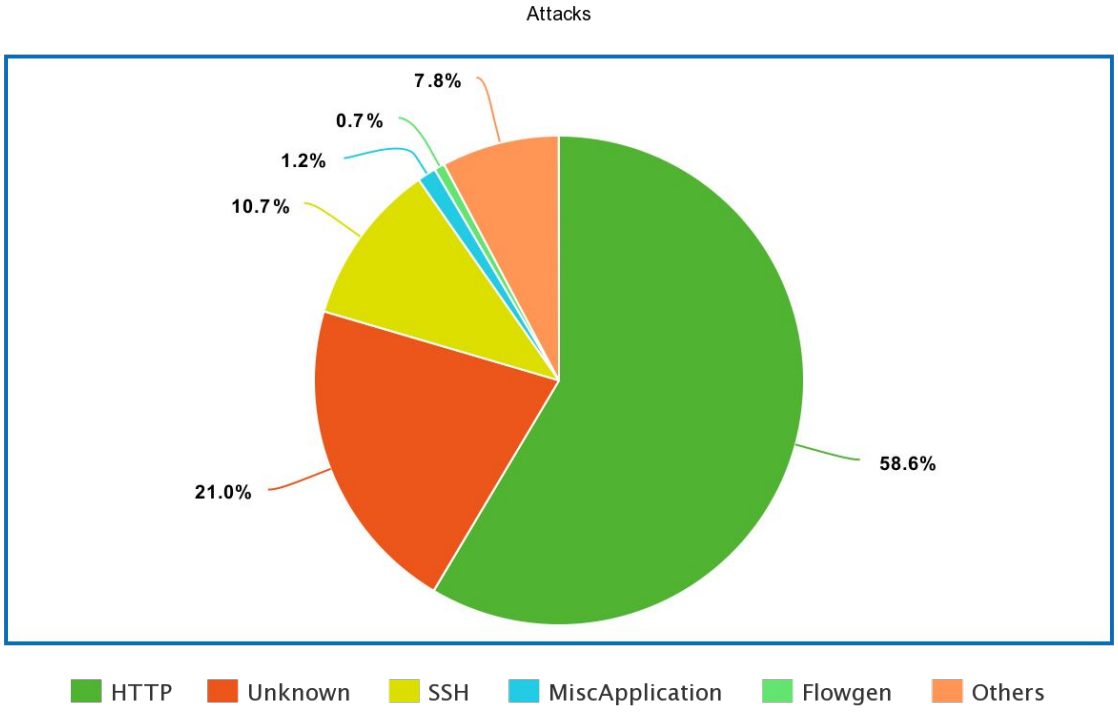
Attack	SMTP	192.168.5.	MjIwIHNlc	220 server	25	F,S,P,A	R2L	tcp_ip	131.202.2	TestbedSu	RUhMTyBi	EHLO back	5096	F,S,P,A	2010-06-1	2010-06-1	1945	22	11917	18
Attack	SMTP	192.168.5.	MjIwIHNlc	220 server	25	F,S,P,A	R2L	tcp_ip	131.202.2	TestbedSu	RUhMTyBi	EHLO back	5096	F,S,P,A	2010-06-1	2010-06-1	1945	22	11917	18
Attack	SecureWe	131.202.2	AGoLAE1a	j.MZ.[REU.	5555	S,P,A	L2R	tcp_ip	192.168.1	TestbedSu	FgMAAFkB	..Y.U.L.-[]N.	54073	S,P,A	2010-06-1	2010-06-1	19592407	43476	28489776	46453
Attack	SecureWe	131.202.2	AGoLAE1a	j.MZ.[REU.	5555	S,P,A	L2R	tcp_ip	192.168.1	TestbedSu	FgMAAFkB	..Y.U.L.-[]N.	54073	S,P,A	2010-06-1	2010-06-1	19592407	43476	28489776	46453
Attack	Tacacs	192.168.1.	-	-	49	-	L2L	tcp_ip	192.168.1	TestbedSu	-	-	34431	S	2010-06-1	2010-06-1	0	0	64	1
Attack	VNC	192.168.1.	-	-	5900	R,A	L2L	tcp_ip	192.168.1	TestbedSu	-	-	34431	S	2010-06-1	2010-06-1	64	1	64	1



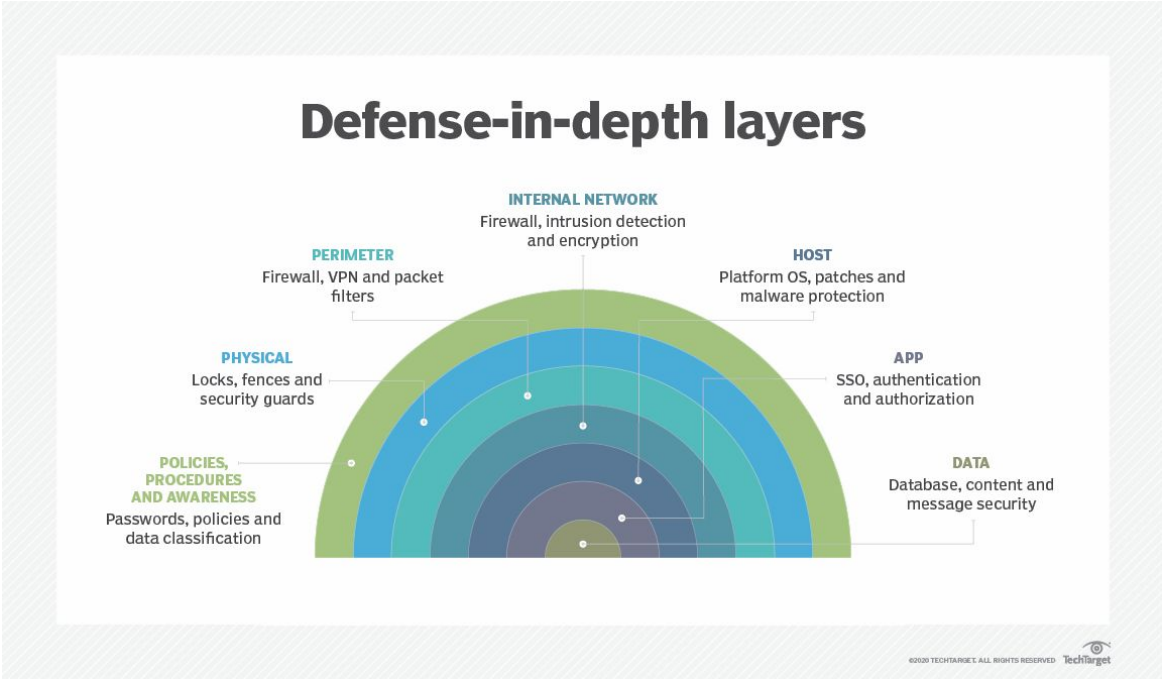
Policy Recommendations



HTTP


Attacks
7.8%
0.7%
1.2%
10.7%
58.6%
21.0%
HTTP
Unknown
SSH
MiscApplication
Flowgen
Others
meta-chart.com

SSH


Defense-in-depth layers
INTERNAL NETWORK
Firewall, intrusion detection and encryption
PERIMETER
Firewall, VPN and packet filters
HOST
Platform OS, patches and malware protection
PHYSICAL
Locks, fences and security guards
APP
SSO, authentication and authorization
POLICIES, PROCEDURES AND AWARENESS
Passwords, policies and data classification
DATA
Database, content and message security
©2020 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

Unknown TCP

- Attacks are made against not commonly used ports
- All unused ports should be blocked

Normal	Unknown_	78.29.44.1	ZDE6cmQ	d1:rd2:id2	35095	-	L2R	udp_ip	192.168.2	TestbedTu	ZDE6YWQ	d1:ad2:id2	58040	-	2010-06-1	2010-06-1	967	4	455	5
Normal	Unknown_	178.130.4.	-	-	46131	-	L2R	udp_ip	192.168.2	TestbedTu	QQLM9MI	A.....[M8..	58040	-	2010-06-1	2010-06-1	0	0	304	4
Normal	Unknown_	98.180.36.	-	-	10500	-	L2R	udp_ip	192.168.2	TestbedTu	QQI+aMLJ	A.>h..A.8..	58040	-	2010-06-1	2010-06-1	0	0	304	4
Normal	Unknown_	79.120.49.	-	-	44807	-	L2R	udp_ip	192.168.2	TestbedTu	ZDE6YWQ	d1:ad2:id2	58040	-	2010-06-1	2010-06-1	0	0	113	1
Normal	Unknown_	90.18.173.	ZDE6cmQ	d1:rd2:id2	12448	-	L2R	udp_ip	192.168.2	TestbedTu	ZDE6YWQ	d1:ad2:id2	58040	-	2010-06-1	2010-06-1	967	4	455	5
Normal	Unknown_	70.112.18.	ZDE6cmQ	d1:rd2:id2	30593	-	L2R	udp_ip	192.168.2	TestbedTu	ZDE6YWQ	d1:ad2:id2	58040	-	2010-06-1	2010-06-1	967	4	455	5
Normal	Unknown_	222.164.8	-	-	51413	-	L2R	udp_ip	192.168.2	TestbedTu	ZDE6YWQ	d1:ad2:id2	58040	-	2010-06-1	2010-06-1	0	0	113	1
Normal	Unknown_	189.61.20	-	-	49816	-	L2R	udp_ip	192.168.2	TestbedTu	QQK3u8Zr	A....k..8..A	58040	-	2010-06-1	2010-06-1	0	0	304	4
Normal	Unknown_	95.167.11	-	-	49975	-	L2R	udp_ip	192.168.2	TestbedTu	QQLygcg1	A....5..8..A	58040	-	2010-06-1	2010-06-1	0	0	304	4

ICMP

- Security professionals often recommend blocking ICMP
- ICMP has helpful uses in network troubleshooting
- Recommend rate limiting ICMP to prevent abnormal ICMP usage

Attack	ICMP	192.168.2.	-	-	0	-	L2L	icmp_ip	192.168.1	TestbedSu	AAAAAAAA	-	0	-	2010-06-1	2010-06-1	0	0	50688	792
Attack	ICMP	192.168.2.	-	-	0	-	L2L	icmp_ip	192.168.1	TestbedSu	AAAAAAAA	-	0	-	2010-06-1	2010-06-1	0	0	50688	792
Attack	ICMP	192.168.5.	-	-	0	-	L2L	icmp_ip	192.168.2	TestbedSu	AAAAAAAA	-	0	-	2010-06-1	2010-06-1	0	0	51712	808
Attack	ICMP	192.168.5.	-	-	0	-	L2L	icmp_ip	192.168.2	TestbedSu	AAAAAAAA	-	0	-	2010-06-1	2010-06-1	0	0	51712	808
Attack	ICMP	192.168.3.	-	-	0	-	L2L	icmp_ip	192.168.2	TestbedM	AAAAAAAA	-	0	-	2010-06-1	2010-06-1	0	0	51712	808

Telnet

- Incredibly vulnerable protocol
- Network traffic is sent in clear text
- Should always be disabled

Attack	Telnet	192.168.2.	-	-	23	R,A	L2L	tcp_ip	192.168.1	TestbedSu	-	-	54817	S	2010-06-1	2010-06-1	64	1	64	1
Attack	Telnet	192.168.2.	-	-	23	R,A	L2L	tcp_ip	192.168.1	TestbedSu	-	-	54817	S	2010-06-1	2010-06-1	64	1	64	1