DARPA Datasets

Table I consolidates information about different attack scenarios in DARPA datasets used in our evaluation.

Table I
DATASETS. STREAMS 1 TO 5 ARE FROM DARPA ENGAGEMENT 3, STREAMS 6 AND 7 ARE FROM DARPA ENGAGEMENT 5. STREAMS 5 CONTAINS TWO INDEPENDENT ATTACK VECTORS OCCURRING ON THE SAME HOST.

Stream No.	Duration	Platform	Scenario No.	Initial Access Technique	Attack Surface
1	0d1h17m	Ubuntu 14.04 (64bit)	1	Drive-by Download	Firefox 42.0
2	2d5h8m	Ubuntu 12.04 (64bit)	2	Drive-by Download	Firefox 42.0 / Trojan / RAT
3	1d7h25m	Ubuntu 12.04 (64bit)	3	Drive-by Download	Firefox 42.0 / Trojan / RAT
4	2d5h17m	FreeBSD 11.0 (64bit)	4	Web Shell	Web Shell / Nginx backdoor / RAT
5	8d7h15m	FreeBSD 11.0 (64bit)	5	Web shell	Nginx backdoor / sudo
			6	Public-Facing	Nginx backdoor
6	0d0h36	Ubuntu 14.04 (64bit)	7	Drive-by Download	Firefox 42.0 / sudo /sshd / Process Inject
7	1d22h58m	Ubuntu 12.04 (64bit)	8	Drive-by Download	Firefox 42.0 / sudo /sshd / Process Inject