Kim Hammar & Rolf Stadler 24 June 2023

Learning Near-Optimal Intrusion Responses Against Dynamic Attackers Supplementary Material
IEEE Transactions on Network and Service Management

Attacker Action Commands

Action	*Command*
TCP SYN scan	`nmap -sS -p- -min-rate 100000 -max-retries 1 -T5 -n`
UDP port scan	`nmap -sU -p- -min-rate 100000 -max-retries 1 -T5 -n`
TCP null scan	`nmap -sN -p- -min-rate 100000 -max-retries 1 -T5 -n`
TCP xmas scan	`nmap -sX -p- -min-rate 100000 -max-retries 1 -T5 -n`
TCP FIN scan	`nmap -sF -p- -min-rate 100000 -max-retries 1 -T5 -n`
Ping scan	`nmap -sP -min-rate 100000 -max-retries 1 -T5 -n`
TCP connection scan	`nmap -sT -p- -min-rate 100000 -max-retries 1 -T5 -n`
Vulscan	`nmap -sV -script=vulscan/vulscan.nse -max-retries 1 -T5 -n`
Telnet-brute force	`nmap -p 23 -script telnet-brute`
SSH brute-force	`nmap -p 22 -script ssh-brute`
FTP brute-force	`nmap -p 21 -script ftp-brute`
Cassandra brute-force	`nmap -p 9160 -script cassandra-brute`
IRC brute-force	`nmap -p 6667 -script irc-brute`
MongoDB brute-force	`nmap -p 27017 -script mongo-brute`
MySQL brute-force	`nmap -p 27017 -script mysql-brute`
SMTP brute-force	`nmap -p 25 -script smtp-brute`
Postgres brute-force	`nmap -p 5432 -script pgsql-brute`
CVE-2017-7494 exploit	`python samba_exploit.py`
CVE-2015-3306 exploit	`python /cve_2015_3306_exploit.py`
CVE-2010-0426 exploit	`/cve_2010_0426_exploit.sh`
CVE-2015-5602 exploit	`/cve_2015_5602_exploit.sh`
CVE-2014-6271 exploit	`/cve_2014_6271_exploit.sh`
CVE-2016-10033 exploit	`/cve_2016_10033_exploit.sh`
CVE-2015-1427 exploit	`/cve_2015_1427_exploit.sh`
Exploit of the CWE-89 weakness on DVWA [5]	`/sql_injection_exploit.sh`

Table 1: Attacker commands executed on the emulation system; actions that exploit vulnerabilities in specific software products are identified according to the corresponding vulnerability identifier in the Common Vulnerabilities and Exposures (CVE) database [1]; actions that exploit vulnerabilities that are not available in the CVE database are identified according to the type of the vulnerability they exploit based on the Common Weakness Enumeration (CWE) list [2]; the Bash and Python scripts that implement the exploits are available at [4].

Defender Action Commands

Stop index	*Action*	*Command*
1	Revoke user certificates	`openssl ca -revoke <certificate>`
2	Blacklist IPs	`iptables -A INPUT -s <ip> -j DROP`
3	Drop traffic that generates IDPS alerts of priority 1	`pulledpork.pl -c /pulledpork/etc/1.conf -l -P -E -H SIGHUP`
4	Drop traffic that generates IDPS alerts of priority 2	`pulledpork.pl -c /pulledpork/etc/2.conf -l -P -E -H SIGHUP`
5	Drop traffic that generates IDPS alerts of priority 3	`pulledpork.pl -c /pulledpork/etc/3.conf -l -P -E -H SIGHUP`
6	Drop traffic that generates IDPS alerts of priority 4	`pulledpork.pl -c /pulledpork/etc/4.conf -l -P -E -H SIGHUP`
7	Block gateway	`iptables -A INPUT -i eth0 -j DROP`

Table 2: Defender commands executed on the emulation system; "Pulledpork" is a software framework for rule management in Snort, for more information see [3].

Client Population Commands

Functions	*Application servers*	*Commands*
HTTP	N_2, N_3, N_{10}, N_{12}	`curl <url>`
SSH	N_2, N_3, N_{10}, N_{12}	`sshpass -p <pw> ssh -oStrictHostKeyChecking=no <hostname>`
SNMP	$N_2, N_3, N_{10}, N_{12}, N_{31}, N_{13}, N_{14}, N_{15}, N_{16}$	`snmpwalk -v2c <hostname>`
ICMP	N_2, N_3, N_{10}, N_{12}	`ping <hostname>`
IRC	$N_{31}, N_{13}, N_{14}, N_{15}, N_{16}$	`./irc_login_test.sh`
Postgres	$N_{31}, N_{13}, N_{14}, N_{15}, N_{16}$	`psql -h <hostname>`
FTP	N_{10}, N_{22}, N_4	`ftp <hostname>`
DNS	N_{10}, N_{22}, N_4	`nslookup <hostname>`
Telnet	N_{10}, N_{22}, N_4	`telnet <hostname>`

Table 3: Emulated client population; each client invokes functions on application servers; the auxillary Bash scripts are available at [4].

References

[1] The MITRE Corporation. Cve database, 2022. https://cve.mitre.org/.

[2] The MITRE Corporation. Cwe list, 2023. https://cwe.mitre.org/index.html.

[3] JJ Cummings and Michael Shirk. Pulledpork, 2023. https://github.com/shirkdog/pulledpork.

[4] Kim Hammar and Rolf Stadler. Supplementary material - learning near-optimal intrusion responses against dynamic attackers, 2023. https://github.com/Limmen/TNSM_Learning_IRS_Supplementary.

[5] The DVWA team. Damn vulnerable web application (dvwa), 2023. https://github.com/digininja/DVWA.