Table 4: Host and Network Attacks

Attack					Impact		
Attack Type	Attack Tool	Interface / Target	Description	MITRE ATT&CK Tactics and Techniques	C	I	A
TCP Port Scan	nmap	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Identify open TCP ports on a target system.	Discovery - Service Discovery (T1007) Network Service Discovery (T1046)	●	○	○
Service Version Detection	nmap	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Determine the software and version running on open ports.	Discovery - Service Discovery (T1007), Software Discovery (T1518)	●	○	○
OS Fingerprinting	nmap	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Attempt to identify the operating system.	Reconnaissance - Gather Victim Host Information (T1595) Discovery - System Information Discovery (T1082)	●	○	○
Aggressive Scan	nmap	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Combine various scan types for a comprehensive view of the target.	Reconnaissance - Gather Victim Host Information (T1595) Discovery - Service Discovery (T1007), Collection (T1119)	●	○	○
SYN Stealth Scan	nmap	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Use SYN packets to identify open ports.	Discovery - Service Discovery (T1007)	●	○	○
Vulnerability Scan	nmap	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Systematically scanning network interface to identify potentially exploitable security flaws.	Reconnaissance - Gather Victim Host Information (T1595) Discovery - System Information Discovery (T1082) Network Service Discovery (T1046)	●	○	○
Slowloris Scan	nmap	EVSE-A: OCPP	Explot local webserver on EVSE by keeping multiple connections, exploit limitations on concurrent connections to exhaust its resources and render it unresponsive.	Impact - Endpoint Denial of Service (T1499)	○	○	●
UDP Flood	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Sends large volumnes of UDP packets to overwhelm targeted network interfaces.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499).	○	○	●
ICMP Flood	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Sends large volumnes of ICMP packets to overwhelm targeted network interfaces.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499)	○	○	●
PSHACK Flood	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Flood attack exploiting the TCP PSH flag to overwhelm targeted network interfaces.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499)	○	○	●
ICMP Fragmentation	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Sending fragmented ICMP packets to exploit vulnerabilities in handling fragmented traffic on the target network interface.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499)	○	○	●
TCP Flood	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Overloading target's network interface with a large volume of TCP packets to disrupt services and cause unresponsiveness.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499)	○	○	●
SYN Flood	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Flooding a target's network interface with a high volume of TCP SYN packets, exploiting the three-way handshake process and causing service disruption.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499)	○	○	●
SynonymousIP Flood	hping3	EVSE-A: OCPP EVSE-B: OCPP & ISO15118	Sending a flood of packets from synonymous IP addresses, potentially evading detection and overwhelming target network interface.	Impact - Network Denial of Service (T1498), Endpoint Denial of Service (T1499)	○	○	●
Cryptojacking	Monero	EVSE-B	Illegitimate use of victim's computing resources to mine cryptocurrency without consent	Impact - Resource Hijacking (T1496)	●	●	●
Backdoor	C2 Server	EVSE-B	Unauthorised remote access to a victim. For our experiment, the C2 server drops and executes malicious scripts on the victim EVSE. Malicious Activities: Payload download, File access permission changes, File encryption and decryption, File creation, deletion and checking PWD.	Execution - Command and Scripting Interpreter (T1059) Command and Control - Content Injection (T1659) Defense Evasion - File and Directory Permissions Modification (T1222), Indicator Remover (T1070) Impact - Data Encrypted for Impact (T1486) Discovery - File and Directory Discovery (T1083)	●	●	●