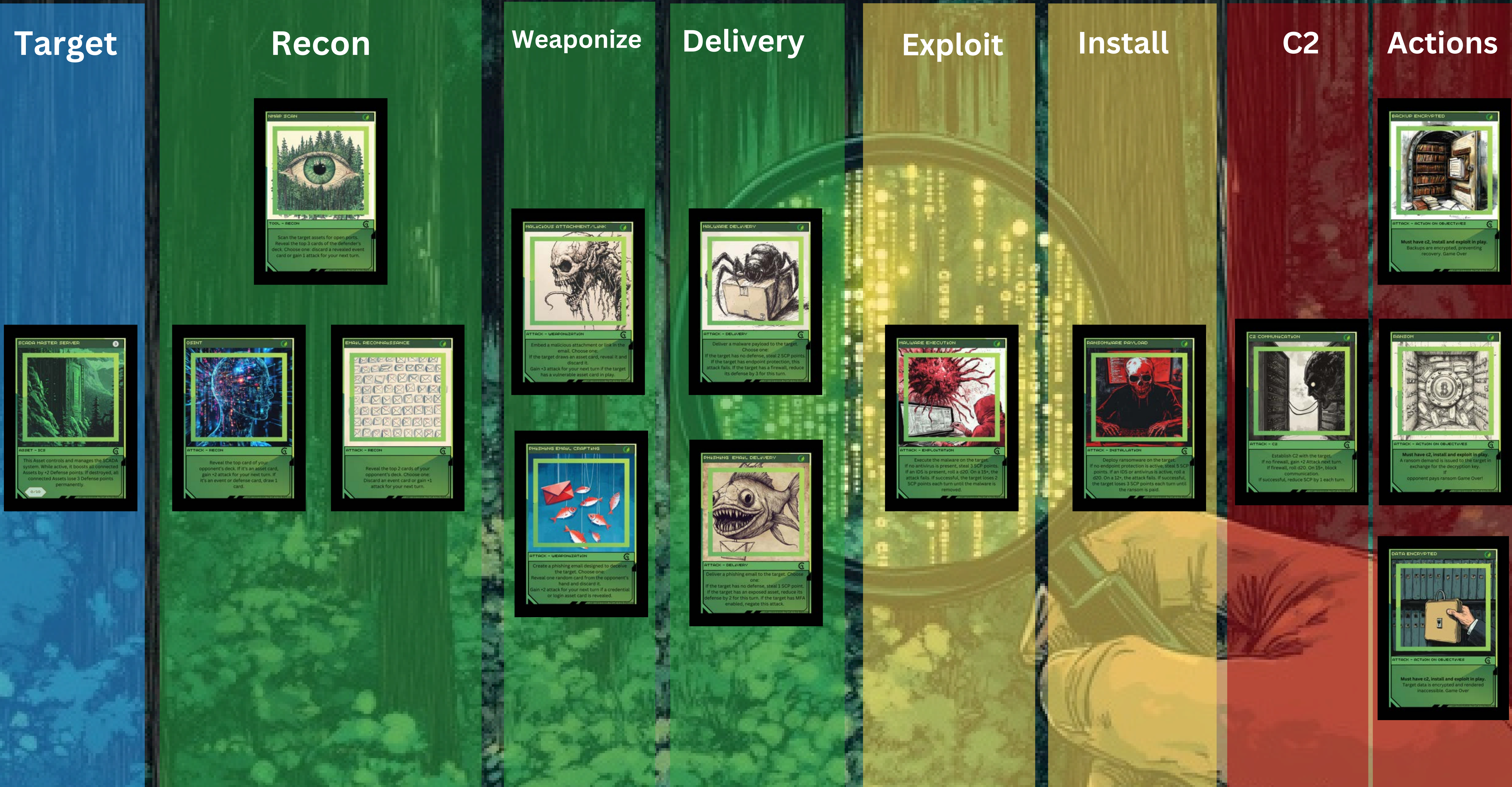


Ransomware Attack

(Cyber Kill Chain)



SSH Attack

(Cyber Kill Chain)

Target	Recon	Weaponize	Delivery	Exploit	Install	C2	Actions
 <p>EXPOSED LINUX SERVER ASSET - ICE</p> <p>An exposed Linux server configured with weak credentials, leaving it vulnerable to unauthorized access. Attackers can exploit its open SSH service on port 2222 to launch brute force attempts.</p>	 <p>SHODAN TOOL - RECON</p> <p>Scan the target assets for open ports. Reveal the top card of the defender's deck and choose to discard or place anywhere in deck or gain 1 attack for your next turn.</p>	 <p>THC HYDRA SETUP TOOL - WEAPONIZE</p> <p>This card sets up the THC Hydra tool for an upcoming brute-force attack. It requires a Recon card to activate. Once in play, the SSH Brute-Force Attack-Delivery card may be played next turn.</p>	 <p>SSH LOGIN EXPLOIT ATTACK - EXPLOIT</p> <p>Requires SSH Brute Force in play. Roll a dice against the defender. If you win, gain full access to the Exposed Linux Server and reduce its defense to 0. If you lose, the defender may draw 1 card as a countermeasure.</p>	 <p>UNAUTHORIZED ACCESS GAINED TOOL - EXPLOIT</p> <p>Requires SSH Login Exploit to be successful. Gain access to the Exposed Linux Server. If you draw the Backdoor Installation card later, you can install a backdoor. If not, continue with other actions but maintain access.</p>	 <p>BACKDOOR INSTALLATION ATTACK - INSTALLATION</p> <p>Install a persistent backdoor on the target asset if Unauthorized Access Gained is in play. Roll Dice. Higher roll succeeds, lower roll fails. If successful, maintain access to the system and can perform further actions.</p>	 <p>MAINTAINS SSH ACCESS ATTACK - COMMAND & CONTROL (C2)</p> <p>Secure persistent access to the compromised system. Roll dice: higher roll grants persistent access, lower roll fails. Requires: Backdoor Installation card in play.</p>	 <p>DATA EXFILTRATION ATTACK - ACTIONS ON OBJECTIVES</p> <p>Requires Exploit + Install or C2 this turn. Roll a dice. If your roll is higher than the defender's, discard a random card from the defender's hand and they lose 20 SCP points. If the defender rolls higher, the attack fails, and you may draw 1 card.</p>
 <p>NMAP SCAN TOOL - RECON</p> <p>Scan the target assets for open ports. Reveal the top 3 cards of the defender's deck. Choose one: discard a revealed event card or gain 1 attack for your next turn.</p>	 <p>USERNAME ENUMERATION ATTACK - RECON</p> <p>Scan for valid usernames. Reveal the top card of the defender's hand. If it's a defense or protocol, add 2 attack to your next attack. If it's an operator or event, draw 1 card.</p>	 <p>PASSWORD LIST SETUP TOOL - WEAPONIZE</p> <p>Requires a Recon Card to activate. Prepare a brute-force attack by selecting a wordlist. Reduce the defender's next SSH Brute-Force Attack roll by 2.</p>	 <p>SSH BRUTE-FORCE ATTACK - DELIVERY</p> <p>Perform a brute-force attack if THC Hydra Setup Tool is in play. Roll a Dice and compare with the defender's roll. If your roll is higher, reduce the defense of the exposed Linux server asset by 3. If the defender wins, the attack fails, and you may draw 1 card.</p>	 <p>MIMIKATZ CREDENTIAL DUMPING TOOL - EXPLOIT</p> <p>Requires SSH brute force to be successful. Perform a credential dump on the target. Roll a dice. If your roll is higher than the defender's, gain access to their stored credentials. Discard a random card from the defender's hand.</p>	 <p>WEAK CREDENTIAL EXPLOIT ATTACK - EXPLOIT</p> <p>Target an asset with 2 or less defense. Roll a dice against the defender. If you win, gain full access and reduce the asset's defense to 0. If you lose, the defender may draw 1 card.</p>	 <p>PRIVILEGE ESCALATION ATTACK - INSTALLATION</p> <p>Elevate privileges on the compromised system. Roll Dice. Higher roll succeeds, lower roll fails. Requires: Backdoor Installation card or mimikatz credential dumping in play.</p>	 <p>CREDENTIAL HARVESTING ATTACK - COMMAND & CONTROL (C2)</p> <p>Steal credentials from the defender. Roll a dice: if your roll is higher, gain 3 card from the defender's hand. If the defender wins, discard a card from your hand. Requires: Install card.</p>
	 <p>METASPLOIT RUN SCANNERS TOOL - RECON</p> <p>Scan the target assets for open ports. Reveal the top 2 cards of the defender's deck. Choose one: discard a revealed card or gain 1 attack for your next turn.</p>	 <p>METASPLOIT EXPLOIT SETUP TOOL - WEAPONIZE</p> <p>This card sets up the Metasploit tool for an upcoming brute-force attack. It requires a Metasploit Recon card to activate. Once in play, the SSH Brute-Force Attack-Delivery card may be played next turn.</p>		 <p>METASPLOIT SSH EXPLOIT ATTACK - EXPLOIT</p> <p>Requires SSH Brute Force in play. Roll a dice against the defender. If you win, gain full access to the Exposed Linux Server and reduce its defense to 0. If you lose, the defender may draw 1 card as a countermeasure.</p>	 <p>METASPLOIT PAYLOAD INSTALL ATTACK - INSTALLATION</p> <p>Roll a dice: if higher than the defender's, install the payload and reduce their SCP by 3. If the defender wins, the attack fails, and you draw 1 card. Requires: Metasploit SSH Exploit</p>		 <p>LOG TAMPERING ATTACK - ACTIONS ON OBJECTIVES</p> <p>Requires Exploit + Install or C2 this turn. Roll a dice: if higher than the defender's, asset loses 10 defense points, if lower draw one card.</p>

Data Breach

(Cyber Kill Chain)

