2024 Verizon DBIR Report
Mitre Att&ck Mapped to Incident Classification Patterns

RECONNAISSANCE

- [ ] Active Scanning: T1595 (Basic Web Application Attacks)
- [ ] Vulnerability Scanning: T1595.002 (System Intrusion) (Basic Web Application Attacks)
- [ ] Social Media Accounts: T1586.001 (System Intrusion)
- [ ] Spearphishing Attachment: T1566.001 (Social Engineering)
- [ ] Spearphishing Link: T1566.002 (Social Engineering)
- [ ] Spearphishing via Service: T1566.003 (Social Engineering)
- [ ] Phishing for Information: T1598 (Social Engineering)
- [ ] Spearphishing Service: T1598.001 (Social Engineering)

PERSISTENCE

- [ ] External Remote Services: T1133 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Valid Accounts: T1078 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Default Accounts: T1078.001 (System Intrusion) (Basic Web Application Attacks)
- [ ] Domain Accounts: T1078.002 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Local Accounts: T1078.003 (System Intrusion)
- [ ] Cloud Accounts: T1078.004 (System Intrusion)

CREDENTIAL ACCESS

- [ ] Exploitation for Credential Access: T1212 (System Intrusion)
- [ ] Brute Force: T1110 (Basic Web Application Attacks)
- [ ] Credential Stuffing: T1110.004 (Basic Web Application Attacks)
- [ ] Password Cracking: T1110.002 (Basic Web Application Attacks)
- [ ] Password Guessing: T1110.001 (Basic Web Application Attacks)
- [ ] Password Spraying: T1110.003 (Basic Web Application Attacks)

RESOURCE DEVELOPMENT

- [ ] Compromise Accounts: T1586 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Email Accounts: T1586.002 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Establish Accounts: T1585 (Social Engineering)
- [ ] Email Accounts: T1585.002 (Social Engineering)

PRIVILEGE ESCALATION

- [ ] Exploitation for Privilege Escalation: T1068 (System Intrusion)
- [ ] Valid Accounts: T1078 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Default Accounts: T1078.001 (System Intrusion) (Basic Web Application Attacks)
- [ ] Domain Accounts: T1078.002 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Local Accounts: T1078.003 (System Intrusion)
- [ ] Cloud Accounts: T1078.004 (System Intrusion)

LATERAL MOVEMENT

- [ ] Exploitation of Remote Services: T1210 (System Intrusion)
- [ ] External Remote Services: T1133 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Remote Services: T1021 (System Intrusion)
- [ ] Remote Desktop Protocol: T1021.001 (System Intrusion)
- [ ] Internal Spearphishing: T1534 (Social Engineering)

DISCOVERY

- [ ] Email Accounts: T1586.002 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)

INITIAL ACCESS

- [ ] Exploit Public-Facing Application: T1190 (System Intrusion) (Basic Web Application Attacks)
- [ ] External Remote Services: T1133 (System Intrusion) (Social Engineering)
- [ ] Valid Accounts: T1078 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Default Accounts: T1078.001 (System Intrusion) (Basic Web Application Attacks)
- [ ] Domain Accounts: T1078.002 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Local Accounts: T1078.003 (System Intrusion)
- [ ] Cloud Accounts: T1078.004 (System Intrusion)
- [ ] Phishing: T1566 (Social Engineering)
- [ ] Spearphishing Attachment: T1566.001 (Social Engineering)
- [ ] Spearphishing Link: T1566.002 (Social Engineering)
- [ ] Spearphishing via Service: T1566.003 (Social Engineering)

DEFENSE EVASION

- [ ] Exploitation for Defense Evasion: T1211 (System Intrusion)
- [ ] Use Alternate Authentication Material: T1550 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Application Access Token: T1550.001 (Social Engineering) (Basic Web Application Attacks)
- [ ] Web Session Cookie: T1550.004 (System Intrusion)
- [ ] Valid Accounts: T1078 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Default Accounts: T1078.001 (System Intrusion) (Basic Web Application Attacks)
- [ ] Domain Accounts: T1078.002 (System Intrusion) (Social Engineering) (Basic Web Application Attacks)
- [ ] Local Accounts: T1078.003 (System Intrusion)
- [ ] Cloud Accounts: T1078.004 (System Intrusion)

Source: 2024 Verizon Data Breach Investigations Report

VulnCheck

Volume of CVE's Mapped from VulnCheck to Mitre Attack Techniques in Verizon DBIR

38,487	24,918	15,818	1,033	267	145
Exploitation of Remote Services T1210	Exploit Public-Facing Application T1190	Exploitation for Privilege Escalation T1068	External Remote Services T1133	Password Guessing T1110.001	Password Spraying T1110.003