CYBERQUIZZER CHEAT SHEET

MITRE ATT&CK Enterprise Matrix

All 14 tactics in matrix order — the adversary's **goals**, left to right — each with the techniques you are most likely to meet in the wild and in an exam.

Scan to drill this sheet

THREE IDS **TA0001** **Tactic** — the why. 14 of them. **T1566** **Technique** — the how. **T1566.001** **Sub-technique** — the specific how.

TA0043 Reconnaissance

- **T1595** Active Scanning
- **T1589** Gather Victim Identity Info
- **T1598** Phishing for Information
- **T1590** Gather Victim Network Info

TA0042 Resource Development

- **T1583** Acquire Infrastructure
- **T1588** Obtain Capabilities
- **T1585** Establish Accounts
- **T1608** Stage Capabilities

TA0001 Initial Access

- **T1566** Phishing
- **T1190** Exploit Public-Facing App
- **T1078** Valid Accounts
- **T1133** External Remote Services

TA0002 Execution

- **T1059** Command & Scripting Interpreter
- **T1204** User Execution
- **T1053** Scheduled Task / Job
- **T1569** System Services

TA0003 Persistence

- **T1547** Boot / Logon Autostart
- **T1136** Create Account
- **T1505** Server Software Component
- **T1098** Account Manipulation

TA0004 Privilege Escalation

- **T1068** Exploitation for Priv Esc
- **T1548** Abuse Elevation Control
- **T1055** Process Injection
- **T1134** Access Token Manipulation

TA0005 Defense Evasion

- **T1070** Indicator Removal
- **T1027** Obfuscated Files or Info
- **T1562** Impair Defenses
- **T1218** System Binary Proxy Exec

TA0006 Credential Access

- **T1110** Brute Force
- **T1003** OS Credential Dumping
- **T1555** Creds from Password Stores
- **T1056** Input Capture

TA0007 Discovery

- **T1082** System Information Discovery
- **T1018** Remote System Discovery
- **T1087** Account Discovery
- **T1057** Process Discovery

TA0008 Lateral Movement

- **T1021** Remote Services
- **T1550** Use Alternate Auth Material
- **T1570** Lateral Tool Transfer
- **T1091** Replication via Removable Media

TA0009 Collection

- **T1005** Data from Local System
- **T1114** Email Collection
- **T1056** Input Capture
- **T1560** Archive Collected Data

TA0011 Command & Control

- **T1071** Application Layer Protocol
- **T1105** Ingress Tool Transfer
- **T1573** Encrypted Channel
- **T1090** Proxy

TA0010 Exfiltration

- **T1041** Exfil Over C2 Channel
- **T1048** Exfil Over Alt Protocol
- **T1567** Exfil Over Web Service
- **T1052** Exfil Over Physical Medium

TA0040 Impact

- **T1486** Data Encrypted for Impact
- **T1490** Inhibit System Recovery
- **T1489** Service Stop
- **T1498** Network Denial of Service

Numbers aren't order

TA IDs were assigned as tactics were added, so they don't run in matrix order — C2 is **TA0011** but sits before Exfiltration **TA0010**. Learn the sequence, not the digits.

Where people lose the mark

Three distinctions that decide most ATT&CK questions.

Tactic vs technique

A tactic is the **objective**, a technique is the **method**. "Credential Access" is why; "OS Credential Dumping" is how. One technique can serve several tactics.

ATT&CK vs Kill Chain

The Kill Chain is a **linear sequence** of 7 phases. ATT&CK is a **matrix** of observed behaviour — adversaries revisit tactics, skip them, and run several at once.

Procedure ≠ technique

A procedure is one group's **specific implementation** — "APT29 used PowerShell to dump LSASS". Same technique, many procedures.

Reading the matrix won't stick — turn it into instinct.

Drill tactic-and-technique recall until the ID comes back automatically. Ten minutes a day, free forever, no card.

cyberquizzer.com/go/mitre-sheet

Framework: MITRE ATT&CK® Enterprise · Updated August 2026

© CyberQuizzer