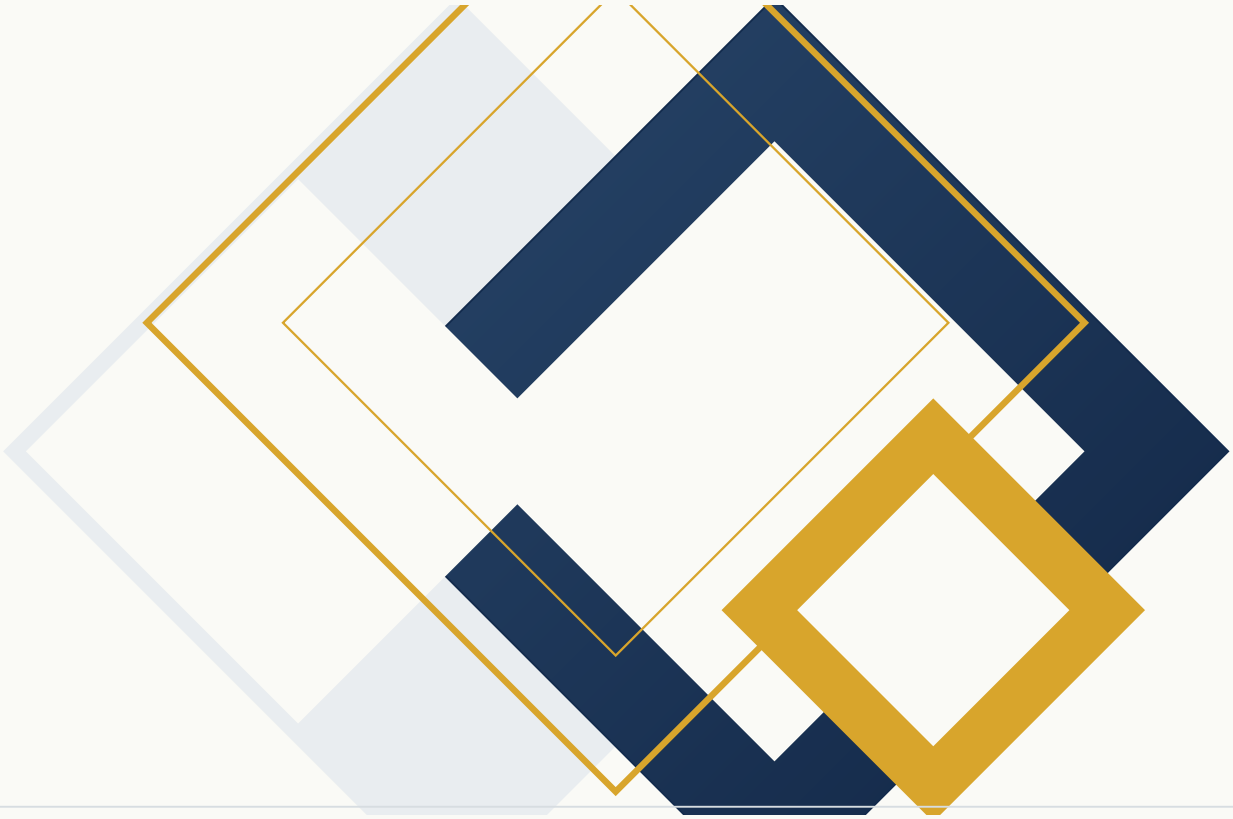
ISECOM

ISECOM PUBLICATIONS

# Jack of All Trades

VERSION 3 / OCTOBER 2026



**ISECOM**

Institute for Security and

Open Methodologies

VERSION HISTORY

3 / October 2026

2 / April 20, 2009

1 / March 19, 2001

# About This Document

Jack of All Trades (JAT) is an instructor-led classroom exercise for teaching security thinking through non-security scenarios. It is not a test to hand out and grade. It is a guided discussion where the instructor uses everyday situations to draw out how students reason about protection, access, trust, verification, and control.

JAT is part of the OSSTMM (Open Source Security Testing Methodology Manual) training program and is used in OPST and OPSA certification courses. It works because security is not a technology discipline. It is a reasoning discipline. The same thinking that protects a building protects a network. The same logic that verifies a patient's identity verifies a user's session. JAT makes that transferable reasoning visible.

The instructor's role is not to grade answers as right or wrong. It is to use the answers as entry points into deeper discussion: why did you think of that? What assumption were you making? What would break if that assumption was wrong?

# How to Use This Document

**Format:** Instructor-led discussion. The instructor reads or paraphrases each scenario aloud and poses the questions. Students answer individually (written, timed) or in open discussion, depending on class size and goals.

**Timing:** 8 to 10 minutes per question when written. Open discussion naturally takes longer. A full session of 4 scenarios runs approximately 90 minutes with debrief.

**Selection:** You do not need to run all scenarios in one session. Choose scenarios that fit the class level and the security concepts you want to surface. The Instructor Notes under each scenario tell you what it is designed to reveal, including which OSSTMM analysis concept it teaches best.

**Debrief:** The debrief after each scenario is where learning happens. Do not skip it. Use the Instructor Notes to connect student answers back to security principles. Ask follow-up questions: "What would change if...?" "What are you trusting when you do that?" "How would you verify that?"

CC BY-NC-ND 3.0 + OML

**Evaluation:** JAT does not produce a score. It produces a picture of how someone thinks about security. Look for:

- **Breadth vs depth.** Does the student generate many surface-level ideas, or fewer ideas with reasoning behind them?
- **Attacker thinking.** Does the student naturally consider how their protections could be defeated?
- **Trust awareness.** Does the student notice where they are making trust assumptions?
- **Operational realism.** Are the student's ideas things that could actually be implemented?

CC BY-NC-ND 3.0 + OML

# Part One: Foundations

These scenarios introduce security reasoning through physical and everyday situations. No technical background required. Suitable for all levels.

## Scenario 1: Electrician

You are an electrician. In front of you is a light hanging from the ceiling. Behind you is a light switch on the wall. The light is currently on.

1. List 10 ways to turn off the light.
2. List 10 components of a functioning light.
3. List 10 ways to verify the light is actually off and not just appearing off.
4. List 10 ways to prevent someone from being able to turn the light back on.

**Evidence Hierarchy (verification vs assumption)**

Q3 is the key question and it teaches the entire evidence hierarchy in miniature. Students who only list visual checks ("look at it") are trusting one channel of observation. They are generating Level 1 evidence: self-reported, single-source. Push them: what if the bulb is behind a wall? What if it is an indicator light and the circuit is still live?

This is the difference between observing a state and verifying a state. In OSSTMM terms, it is the difference between evidence gathered by asking (the light looks off) and evidence gathered by testing (I measured zero voltage across the terminals).

Q1 and Q2 are enumeration exercises. Q1 enumerates the interaction points where you can affect the system. Q2 enumerates the components, which is attack surface mapping. Q4 maps to specific security controls: removing the switch is reducing attack surface, locking the switch is access control, cutting the wire is eliminating the channel entirely.

---

"You just built an evidence hierarchy without knowing it. Your weakest answers to Q3 were 'look at it.' Your strongest were 'test the circuit with a meter.' In security testing, this same range exists: you can ask someone if their firewall works, or you can test the firewall yourself. The methodology cares about which one you did."

CC BY-NC-ND 3.0 + OML

## Scenario 2: Delivery Driver

You are a driver for a logistics company. You have a package to deliver to a residential address. You have never been to this address before.

1. List 10 ways to confirm you have the right recipient.
2. List 10 things that could prevent you from completing the delivery.
3. List 10 reasons a package should be delivered at all rather than returned to sender.
4. List 10 ways to verify the identity of the sender.

**Trust Properties**

Q1 is identity verification. Students who list "ask their name" are using single-factor authentication. Those who combine name, ID, address, and expectation of delivery are layering trust verification across multiple properties: consistency, completeness, and transparency.

The delivery driver is a trust proxy. The sender trusts the driver to deliver correctly. The recipient trusts the driver to have a legitimate package. But neither trusts the other directly. The driver mediates trust between parties with no direct relationship.

Q4 flips the direction: verifying the source, not the destination. Students who breeze through Q1 but struggle with Q4 are revealing a common blind spot. Upstream trust matters as much as downstream authentication.

---

"Trust in this scenario has properties you can name and test. Is the trust between sender and driver symmetric? Is it transparent? What happens when one property fails but others hold? These are measurable qualities of a trust relationship, not just a feeling."

CC BY-NC-ND 3.0 + OML

## Scenario 3: Landlord

You own a small apartment building with six units. A new tenant is moving in.

1. List 10 things you need to verify about the new tenant before giving them keys.
2. List 10 ways the tenant could compromise the security of the building for other tenants.
3. List 10 responsibilities you have for maintaining the security of the building.
4. List 10 ways a former tenant who still has a key could cause problems.

**Trust Lifecycle (provisioning through revocation)**

The arc from Q1 to Q4 IS the trust lifecycle. Q1 is trust establishment. Q3 is trust maintenance. Q4 is trust revocation failure: what happens when access persists after the trust relationship ends.

The gap between provisioning and revocation is where most access-control failures actually occur. Organizations are generally better at granting access than revoking it.

**Trust/Privacy Inverse (strong fit):** Q1 is the clearest example. Verifying a new tenant requires accessing their financial history, employment records, references, and identity documents. The tenant must sacrifice privacy to establish trust. This is the fundamental mechanism by which trust operates.

---

"You just mapped a trust lifecycle: establish, maintain, revoke. Most security programs invest heavily in step one and barely think about step three. The landlord who never changes the locks after a tenant leaves has the same problem as the IT department that never disables accounts after an employee departs."

CC BY-NC-ND 3.0 + OML

## Scenario 4: Doctor

You are a doctor in a walk-in clinic. A parent brings in a child who is unresponsive.

1. List 10 things you need to assess before beginning treatment.
2. List 10 ways to determine what happened to the child without the parent's account.
3. List 10 precautions you must take to protect yourself and the child during examination.
4. List 10 ways to verify the parent's account of what happened is accurate.

**Independent Evidence vs Self-Attestation**

Q2 is the heart of this scenario. The parent's account is self-attestation. It may be accurate, incomplete, mistaken, or deliberately false. The doctor cannot know which without independent evidence: physical examination, toxicology, medical history, witnesses, injury patterns.

This maps directly to security testing. When a vendor says their product blocks attacks, that is self-attestation. When an internal team says they patched the vulnerability, that is self-attestation. Only independent testing produces verified evidence.

Q4 extends this: the person reporting the incident and the person responsible may be the same person. In security, this is the insider threat.

---

"The doctor who treats based only on what the parent says is the security team that accepts the vendor's compliance certificate without testing. Q2 asked you to find evidence that does not come from the interested party. That distinction is the single most important concept in security assessment."

CC BY-NC-ND 3.0 + OML

# Part Two: Operations

These scenarios introduce more complex reasoning about systems, processes, and adversarial thinking. Suitable for mid-level and above.

## Scenario 5: Soldier

You are a soldier stationed at the only bridge crossing a river gorge. You expect hostile forces from the other side.

1. List 10 ways to prepare your position before the enemy arrives.
2. List 10 ways to prevent the enemy from crossing the bridge.
3. List 10 ways to distinguish friendly civilians from enemy combatants.
4. List 10 consequences of destroying the bridge entirely.

**Controls Taxonomy**

Q2 is the best teaching question. Each answer maps to a specific type of security control. "Block the bridge with barriers" is Channeling. "Post sentries" is Surveillance. "Require identification" is Authentication. "Limit crossing to certain hours" is Throttling.

Q3 is authentication under adversarial conditions. The enemy is actively trying to appear friendly. This is social engineering and impersonation.

Q4 is the trade-off question. Destroying the bridge eliminates the threat channel completely but also eliminates your own access, supply lines, and future flexibility. Every firewall rule that blocks a port also blocks legitimate traffic on that port.

---

"Each of your answers to Q2 was a specific type of control. You intuitively sorted them into surveillance, authentication, access restriction, and channel management. The methodology names these categories because a defense built from only one type of control has a predictable weakness."

CC BY-NC-ND 3.0 + OML

## Scenario 6: Safety Inspector

You are a licensed safety inspector called to a factory after a series of workplace accidents.

1. List 10 questions you would ask the factory foreman in your first hour.
2. List 10 things you would physically inspect without asking anyone.
3. List 10 changes that would make the factory safer that the workers would resist.
4. List 10 ways management could make the accident record look better without actually improving safety.

**Evidence Hierarchy (self-report vs independent testing)**

Q1 and Q2 teach the evidence hierarchy through direct contrast. Q1 gathers evidence by asking. Q2 gathers evidence by looking. The gap between these two sets of answers is the gap between compliance and actual security.

Q3 introduces the human element: security controls that users resist get bypassed. Shadow IT, password workarounds, propping open fire doors. A control that works perfectly but that people route around is not a working control.

Q4 is explicitly about gaming metrics. Reclassify accidents. Underreport near-misses. Change definitions. Each makes the safety record improve on paper while the factory remains exactly as dangerous.

---

"Q1 and Q2 were the same investigation using two different evidence sources. Everything you learned from Q1 came from the foreman. Everything from Q2 came from your own observation. When those disagree, which one do you trust? That question is the entire argument for evidence-based security testing."

CC BY-NC-ND 3.0 + OML

## Scenario 7: Building Inspector

You are a bridge and building inspector for a major city. You must assess an aging bridge for safety.

1. List 10 structural areas you would inspect.
2. List 10 concerns the city would have about shutting the bridge for inspection.
3. List 10 ways the bridge could fail that would not be visible from a surface inspection.
4. List 10 things you would need to verify about the last inspection report before trusting it.

**Evidence Decay**

Q4 introduces the principle that evidence has a shelf life. A previous inspection report is like a previous penetration test report. Before trusting it: How old is it? Who performed it? What methodology? What was in scope? What has changed since?

A report that says "safe" is a statement about a specific moment in time. Every day after, the evidence decays. The environment changes and the evidence has not been refreshed. Security evidence works the same way.

Q3 reinforces from a different angle: hidden failure modes. Internal corrosion, fatigue cracks in load-bearing members. These map to vulnerabilities that do not show up in external scans or compliance reviews. Surface inspection generates surface evidence.

---

"Every answer you gave for Q4 was a reason the previous report might no longer be true. That is evidence decay. The report was accurate when it was written. Time made it less accurate. A penetration test is not a certificate. It is a snapshot."

CC BY-NC-ND 3.0 + OML

## Scenario 8: Mechanic

You are a mechanic at an automotive shop. A customer brings in a used car they are considering purchasing and wants your professional assessment.

1. List 10 questions you would ask the seller about the car.
2. List 10 things you would inspect that the seller is unlikely to mention.
3. List 10 signs that the car's history has been misrepresented.
4. List 10 reasons the buyer should get a second independent inspection.

**Assessment Independence**

Q4 is the payoff: why does the buyer need a second opinion? Because every assessment carries the assessor's biases, blind spots, methodology, and relationship to the parties. A single mechanic might miss something, have a financial incentive, or be competent in one area but weak in another.

Separation of tester from implementer is not a procedural formality. It is an evidence-quality requirement.

Q1 vs Q2 reinforces the evidence hierarchy. Q1 is what the seller volunteers. Q2 is what you find independently. Q3 is detecting deception in self-reported information: the automotive equivalents of falsified compliance evidence.

---

"Q4 asked why one assessment is not enough. Every reason you listed was a form of the same principle: no single assessor can guarantee completeness, and any assessor with a relationship to the outcome has a potential bias. Independence in assessment is not distrust. It is methodology."

CC BY-NC-ND 3.0 + OML

# Part Three: Adversarial Thinking

These scenarios ask students to think as an attacker, a manipulator, or an exploiter. Suitable for advanced students and practitioners.

## Scenario 9: Thief

You are a professional diamond thief who works alone at night.

1. List 10 ways to choose the best target.
2. List 10 security measures you would expect to encounter.
3. List 10 things you would do to avoid detection during the job.
4. List 10 ways to increase the value of what you take from each job.

**Five-Point Process (5PP) from the attacker's perspective**

The attacker's workflow IS the tester's workflow viewed from the other side. Q1 is target selection and scoping. Q2 is reconnaissance and enumeration. Q3 is operational execution with detection avoidance. Q4 goes beyond the initial operation into post-exploitation.

Q1: Students who list "most valuable inventory" think about asset value. Those who list "weakest security" think about vulnerability. Those who list "best ratio of value to risk" think about operational efficiency. The best answers combine all three.

---

"You just walked through a security test from the attacker's side. Q1 was scoping. Q2 was enumeration. Q3 was execution. Q4 was exploitation. The methodology formalizes this same workflow, because understanding how an attacker operates is how you learn to test defenses."

CC BY-NC-ND 3.0 + OML

## Scenario 10: Con Artist

You need to gain access to a private event at a hotel where you are not on the guest list. You have no invitation, no badge, and no contact inside.

1. List 10 ways to get into the event.
2. List 10 things you would observe from outside before attempting entry.
3. List 10 things that could go wrong during your attempt.
4. List 10 ways the event organizer could have prevented your entry.

**Five-Point Process (reconnaissance) and Trust/Privacy Inverse**

Q2 is pure reconnaissance and the strongest 5PP teaching moment. The best attackers spend more time observing than acting. Staff rotation patterns, badge checking consistency, service entrance traffic, which doors are propped open.

Each observation invades the event's operational privacy. The event's security relies partly on its procedures not being visible to outsiders. The more the con artist observes, the weaker the defenses become.

Q4 flips to defense: the round-trip from attack to defend is the core of security testing. But it also surfaces the defender's dilemma: preventing the con artist requires being less open, more restrictive. The defenses that block the attacker also make the event less welcoming for legitimate guests.

---

"Q2 was reconnaissance. Everything you learned by watching made your attack more likely to succeed. The event's security depended partly on you NOT having that information. That relationship, where your increased knowledge reduces their security, is built into how trust and privacy interact."

CC BY-NC-ND 3.0 + OML

## Scenario 11: Smuggler

You need to move a small, valuable object across a national border. The object is legal to possess but the border authority will confiscate it if they find it.

1. List 10 ways to conceal the object during crossing.
2. List 10 things border security will check during inspection.
3. List 10 ways to cross without being inspected at all.
4. List 10 ways a border authority could detect your concealment after the fact.

**Bypass vs Evasion**

Q3 is the most important question. Q1 asks how to defeat the control (evasion). Q3 asks how to avoid the control entirely (bypass). These are fundamentally different operations.

Evasion means you interact with the control and attempt to pass through undetected. Bypass means you find a path where the control does not exist. In almost every real-world scenario, bypass is easier, because it means finding a gap in coverage rather than defeating detection capability.

In security terms: Q1 is evading a firewall rule. Q3 is finding an unmonitored path that does not pass through the firewall at all.

Q4 introduces forensic thinking. Even if the smuggler succeeds, can the defender reconstruct what happened after the fact? A control that does not prevent an action but creates evidence of it is still a control.

---

"Q1 and Q3 taught you the difference between evasion and bypass. Evasion defeats a control. Bypass avoids it. When testing security, finding a bypass is usually more significant, because it means the control had a coverage gap."

CC BY-NC-ND 3.0 + OML

# Part Four: Systems Thinking

These scenarios involve complex environments with multiple stakeholders, trade-offs, and competing priorities. Suitable for senior practitioners and leadership.

## Scenario 12: School Principal

You are the principal of a public school. A series of thefts has occurred from students' lockers.

1. List 10 possible causes of the thefts beyond "someone is stealing."
2. List 10 measures you could take that would reduce theft without making the school feel like a prison.
3. List 10 ways your anti-theft measures could be misused or create new problems.
4. List 10 things you would need to explain to parents about why zero theft is not a realistic goal.

**RAV (proportional measurement of security)**

Q1 forces root-cause thinking. In security, the presenting incident is often not the real problem. Measurement starts with correct diagnosis.

Q2 is about proportional controls. The principal could install cameras everywhere and search every backpack. That would reduce theft and destroy the learning environment. The measure of a control is not just its effectiveness but its cost relative to what it protects. This is the RAV concept: security is a ratio, not an absolute.

Q3 teaches that controls are attack surface too. Cameras become surveillance tools. Monitoring creates data that can be leaked or misused. Every control introduces new risks.

Q4 is communicating risk to non-technical stakeholders. Absolute security does not exist. The ability to explain that honestly is a leadership skill every CISO needs.

"Q2 was about proportional controls. Q3 was about the cost of those controls. Q4 was about communicating what is realistically achievable. Security measurement accounts for all three."

CC BY-NC-ND 3.0 + OML

### Scenario 13: Event Planner

You are organizing a public outdoor concert for 5,000 people.

1. List 10 things that could go wrong that are not related to the performers or the music.
2. List 10 ways you would control who enters and exits the venue.
3. List 10 pieces of information you would need about each vendor working the event.
4. List 10 things you would do differently if you learned a credible threat had been made against the event.

**Controls (Channeling) and Third-Party Trust**

Q2 is Channeling at scale. With 5,000 people, you cannot individually authenticate each one. You must create controlled flow: entry points, exit points, perimeter barriers, credential checks at chokepoints. The number of entry points and their verification requirements determine both security and usability.

Q3 is third-party trust assessment. Vendors are your supply chain. They have physical access. What do you need to know about each one?

Q4 introduces threat-informed posture adjustment. Students who add evacuation planning, communication protocols, and law enforcement coordination are thinking about response and resilience, not just prevention.

"Q2 was about Channeling. Q3 was about trusting your supply chain. Q4 was about adjusting posture when the threat changes. The Channeling decisions from Q2 constrain your response options in Q4, and the vendor trust from Q3 determines whether your supply chain is part of your defense or part of your exposure."

## Facilitator Reference: Mapping to OSSTMM Concepts

Each scenario exercises specific OSSTMM analysis concepts. Use this table to select scenarios based on what you want to teach.

CC BY-NC-ND 3.0 + OML

| OSSTMM Concept | Primary Scenario(s) | Supporting Scenario(s) |
|---|---|---|
| Evidence Hierarchy | 1 (Electrician), 6 (Safety Inspector) | 4 (Doctor), 8 (Mechanic) |
| Trust Properties | 2 (Delivery Driver) | 3 (Landlord), 10 (Con Artist) |
| Trust Lifecycle | 3 (Landlord) | 2 (Delivery Driver) |
| Trust/Privacy Inverse | 3 (Landlord), 4 (Doctor), 10 (Con Artist) | 2 (Delivery Driver), 8 (Mechanic) |
| Controls Taxonomy | 5 (Soldier) | 1 (Electrician), 13 (Event Planner) |
| Five-Point Process (5PP) | 9 (Thief), 10 (Con Artist) | 6 (Safety Inspector), 7 (Building Inspector) |
| Evidence Decay | 7 (Building Inspector) | |
| Assessment Independence | 8 (Mechanic) | 4 (Doctor) |
| Bypass vs Evasion | 11 (Smuggler) | |
| RAV / Proportional Measurement | 12 (School Principal) | 5 (Soldier) |
| Metrics Gaming / False Assurance | 6 (Safety Inspector) | 7 (Building Inspector) |
| Risk Communication | 12 (School Principal) | 13 (Event Planner) |
| Channeling | 13 (Event Planner) | 5 (Soldier) |
| Third-Party / Supply Chain Trust | 13 (Event Planner) | 8 (Mechanic) |
| Second-Order Effects of Controls | 12 (School Principal) | 6 (Safety Inspector) |

**Copyleft Notice**

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License (CC BY-NC-ND 3.0) and the Open Methodology License (OML).

You are free to share, copy, and redistribute this material in any medium or format under the following terms: you must give appropriate credit to ISECOM, you may not use the material for commercial purposes, and you may not distribute modified versions of this material.

The full text of the CC BY-NC-ND 3.0 license is available at https://creativecommons.org/licenses/by-nc-nd/3.0/ and the Open Methodology License at https://www.isecom.org/oml.html

© 2000–2026 ISECOM — Institute for Security and Open Methodologies. All rights reserved.

Research and development maintained by ISECOM. Contact www.isecom.org for licensing questions.