aracne

Classificazione Decimale Dewey:

005.8 (23.) SICUREZZA DEI DATI

GERARDO IOVANE

RED TEAM CYBERSECURITY LECTURES

0-CLICK VULNERABILITIES FOR OPENING SYSTEMS, APPLICATIONS AND CLOUDS

aracne

aracne

©

ISBN
979-12-218-1994-6

PRIMA EDIZIONE
ROMA 6 GIUGNO 2025

Table of contents

Preface

In an increasingly interconnected world, vulnerabilities represent the silent Achilles' heel of every digital infrastructure. Understanding, categorizing, and mitigating these vulnerabilities is no longer an option—it is a necessity.

This book of Cybersecurity Vulnerabilities: Operating Systems, Applications, and Cloud, was born from the need to offer a systematic and comprehensive guide to understanding vulnerabilities across all major platforms. Using the MITRE ATT&CK framework as a guiding thread, this work provides both theoretical knowledge and practical insights, making it a valuable resource for cybersecurity professionals, researchers, system administrators, developers, and students.

The book is organized to mirror real-world operational environments: from Cloud infrastructures to the main families of operating systems, down to specific application vulnerabilities. Each section is structured methodically to ease consultation, study, and field application.

To enhance the analysis, we introduce a dual classification:

- *Vertical Classification*: by platform and application type.
- *Horizontal Classification*: by attack lifecycle phases, based on the MITRE ATT&CK Tactics (Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact).

Our aim is to transform complexity into clarity, and threats into challenges to be anticipated and neutralized.

Welcome to your journey into the critical world of cybersecurity vulnerabilities.

1. Introduction

In the modern world, where digitalization touches every aspect of human activity, cybersecurity has emerged as a critical domain influencing individuals, corporations, governments, and the global economy alike. As technological systems grow more interconnected, the vulnerabilities that permeate software, hardware, and organizational practices become increasingly significant vectors of risk. Vulnerabilities are the silent and often invisible cracks within the infrastructure, waiting to be exploited by malicious actors. Understanding these vulnerabilities is essential not just for cybersecurity professionals, but for anyone engaged in developing, maintaining, or utilizing technology.

The concept of a vulnerability is deceptively simple yet profoundly complex. It represents a weakness or flaw in a system that can be exploited to compromise the confidentiality, integrity, or availability of the information or operations it supports. However, the reality of identifying, classifying, and mitigating vulnerabilities involves an intricate interplay of technical, human, and procedural elements. This complexity necessitates a systematic and methodical approach to studying vulnerabilities — an approach that blends theoretical knowledge with practical, actionable insight. Throughout this work, we aim to provide a structured and comprehensive atlas of cybersecurity vulnerabilities. We will delve into the weaknesses present in different environments: cloud infrastructures, operating systems (across Windows, Linux, macOS, Android, and iOS), and applications running on these platforms. In addition to a vertical classification — organized by platform — we adopt a horizontal perspective aligned with the MITRE ATT&CK framework, mapping vulnerabilities to the stages of an attack lifecycle. This dual approach enables a multi-dimensional understanding that mirrors the complexities encountered in real-world cybersecurity scenarios.

Recognizing the significance of vulnerabilities requires a broader understanding of the threat landscape. The cybersecurity domain does not exist in a vacuum; it is shaped by evolving tactics, techniques, and procedures (TTPs) employed by threat actors. These TTPs often pivot around exploiting vulnerabilities at various stages of an attack — from reconnaissance and initial access to lateral movement, persistence, and eventual exfiltration or sabotage. By systematically categorizing vulnerabilities in alignment with attack phases, security practitioners can better anticipate potential exploitation paths and prioritize defensive measures accordingly.

The scale and diversity of vulnerabilities have expanded dramatically over the past two decades. Early cyberattacks primarily focused on exploiting flaws in individual software applications or operating systems. Today, however, the attack surface encompasses a wide array of interconnected devices, cloud services, mobile platforms, and even IoT ecosystems. This expansion has been accompanied by an exponential growth in the volume of identified vulnerabilities. For instance, the National Vulnerability Database (NVD) reports thousands of new vulnerabilities annually, covering everything from kernel exploits to application misconfigurations and human-centered social engineering attacks.

Compounding the challenge, not all vulnerabilities are created equal. Some are trivial to exploit and can lead to catastrophic consequences, while others may require sophisticated chains of actions and specific preconditions. The Common Vulnerability Scoring System (CVSS) offers a quantitative model for assessing the severity of vulnerabilities, yet effective vulnerability management requires not only understanding the score but also appreciating the broader operational context. Factors such as asset criticality, threat actor motivation, and exposure level must be considered when prioritizing vulnerabilities for remediation.

The MITRE ATT&CK framework provides a foundational structure to organize this understanding. ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary behavior, based on real-world observations. It categorizes cyberattack activities into tactics (the goals), techniques (the methods), and procedures (the detailed implementations). Mapping vulnerabilities to these tactics and techniques allows organizations to visualize how specific weaknesses can be leveraged within the broader kill chain of an attack. This mapping is particularly crucial for designing threat detection and response mechanisms.

Importantly, vulnerabilities are not static entities. Their criticality can evolve over time as new exploit techniques are developed or as their operational context changes. A vulnerability once considered low-risk may become a top priority if a reliable exploit becomes publicly available, or if a critical system suddenly becomes exposed to the internet. This dynamic nature underscores the need for continuous vulnerability management, rather than treating vulnerability scanning and patching as one-time events.

Moreover, the cybersecurity community has recognized that vulnerabilities are not solely the result of technical flaws. Misconfigurations, lack of security hygiene, inadequate access control, and even human error play significant roles in introducing vulnerabilities into systems. Organizational policies and practices must therefore align closely with technical controls to ensure a comprehensive security posture.

The increasing adoption of cloud computing further complicates the vulnerability landscape. While cloud providers implement robust security measures, the shared responsibility model places significant obligations on customers to secure their configurations and applications. Misconfigured storage buckets, exposed API keys, overly permissive identity and access management (IAM) policies, and unpatched container images represent common vulnerability vectors within cloud environments. Each cloud platform — AWS, Azure, GCP — presents its own nuances in vulnerability management, necessitating platform-specific expertise. Mobile platforms, notably Android and iOS, bring another layer of complexity. Unlike traditional operating systems, mobile environments are tightly coupled with application ecosystems, app stores, and user-permitted access controls. Vulnerabilities in mobile apps, operating system permissions, and communication protocols create opportunities for privacy breaches, financial fraud, surveillance, and other threats. Android's more open ecosystem leads to distinct vulnerabilities compared to the more controlled, but still vulnerable, Apple ecosystem.

On the enterprise side, Windows and Linux operating systems remain the backbone of most organizational infrastructures. Both have matured considerably over the decades, yet vulnerabilities continue to surface, often with critical implications. Windows environments face threats like privilege escalation via outdated drivers, Active Directory abuses, and credential dumping, while Linux systems contend with privilege escalation exploits, misconfigurations in sudoers or cron jobs, and vulnerabilities in widely-used services like SSH and web servers.

Applications themselves are fertile grounds for vulnerabilities, whether they run on cloud platforms, desktops, or mobile devices. Injection vulnerabilities, improper authentication, insecure communications, and flawed authorization mechanisms are among the recurring patterns that plague software products across industries. Open-source components, while invaluable, introduce supply chain risks, making software composition analysis a vital aspect of vulnerability management. Beyond the technical realm, vulnerabilities exist at the human and organizational levels. Phishing attacks, social engineering, poor password practices, and negligence all contribute to exposing critical systems. Technical defenses must therefore be complemented by user education, organizational policies, and proactive monitoring to detect anomalies indicative of human-centered attacks.

Another dimension to consider is the attacker's perspective. Skilled adversaries often combine multiple vulnerabilities to create chained attacks that bypass individual security measures. This trend emphasizes the need for defense-in-depth strategies that layer multiple protections, reducing the likelihood that a single exploited vulnerability will lead to system compromise.

Vulnerability disclosure processes also play a critical role in the cybersecurity ecosystem. Coordinated vulnerability disclosure (CVD) frameworks, bug bounty programs, and responsible reporting mechanisms incentivize researchers to report vulnerabilities ethically rather than allowing them to be exploited maliciously. Nevertheless, the existence of gray markets for zero-day vulnerabilities — those not yet publicly disclosed or patched — highlights the ongoing tension between offense and defense in the cybersecurity arms race.

In constructing this book, we will integrate insights from multiple authoritative sources. Besides the MITRE ATT&CK framework, we reference the NIST National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE) system, Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification (CAPEC), OWASP guidelines for web application security, and best practices issued by incident response organizations such as FIRST. This integration ensures that our analysis remains anchored in recognized standards while remaining accessible and actionable.

By following a systematic path through this book, readers will develop a granular understanding of the threat surface that vulnerabilities present. More importantly, they will be better equipped to anticipate, defend against, and ultimately reduce the risk posed by vulnerabilities within their operational environments.

This introduction has laid the groundwork for the exploration that follows. We now proceed to deepen our understanding, starting with the fundamental definition and nature of cybersecurity vulnerabilities.

1.1 Definition of a Cybersecurity Vulnerability

The term "vulnerability" occupies a foundational role in the lexicon of cybersecurity, yet it defies simplistic or monolithic definition. Within its apparent conceptual simplicity lies a multifaceted and dynamic phenomenon, shaped by technical intricacies, systemic interdependencies, human behaviors, and organizational processes. To define a cybersecurity vulnerability with the precision it demands requires an exploration of its ontological nature, operational significance, and evolving manifestations across diverse technological and social contexts. At its core, a cybersecurity vulnerability can be defined as a weakness, flaw, or misconfiguration in an information system, software, hardware, or associated human process that, when exploited, can compromise the confidentiality, integrity, or availability (the CIA triad) of the system or the data it processes. This triad — confidentiality, integrity, and availability — serves as the fundamental model for information security, and any compromise therein constitutes a breach of security. However, a definition purely anchored in the CIA triad risks being overly reductionist. In the complex and adversarial landscape of modern cyberspace, vulnerabilities can also enable violations of authenticity, non-repudiation, accountability, and privacy — attributes that extend beyond the traditional triad. Consequently, a richer, more encompassing definition recognizes that a cybersecurity vulnerability is any condition that introduces an unacceptable level of risk, whether through unauthorized disclosure, alteration, destruction, or misuse of information or systems.

Vulnerabilities may stem from a wide array of sources. At the technical level, they often arise from errors in software code, insecure default configurations, unpatched systems, or poorly designed network protocols. At the human level, they manifest through weak passwords, social engineering susceptibility, lack of security awareness, or improper procedural adherence. At the organizational level, vulnerabilities may emerge from inadequate security governance, absence of incident response plans, insufficient investment in cybersecurity resources, or cultural attitudes that deprioritize security.

The classification and taxonomy of vulnerabilities have evolved significantly, especially in the context of formal frameworks such as the Common Weakness Enumeration (CWE) and the

MITRE ATT&CK knowledge base. CWE categorizes vulnerabilities based on the type of flaw — for example, buffer overflows, injection flaws, and improper access controls — offering a systematic approach to understanding how vulnerabilities are introduced during software development or system configuration. MITRE ATT&CK, conversely, emphasizes the exploitation aspect, categorizing adversarial behaviors that leverage vulnerabilities at various stages of an attack.

A critical dimension to understanding cybersecurity vulnerabilities is their relationship with threats and risks. A vulnerability by itself does not constitute a threat; it is merely a potential that may or may not be realized. A threat is the agent or actor — whether a cybercriminal, nation- state, hacktivist, insider, or automated malware — that can exploit a vulnerability to achieve malicious objectives. Risk, in turn, is the intersection of vulnerability, threat likelihood, and impact severity. Thus, vulnerability management is inherently a risk management discipline, requiring continual assessment of threat dynamics and business context. Furthermore, vulnerabilities are distinguished from weaknesses and exposures; these terms are often used interchangeably but with important nuances. A weakness is a broader term that encompasses any aspect of a system that deviates from security best practices or design principles, while an exposure refers to the presence of a system asset being accessible or observable by a potential adversary. A vulnerability represents a weakness that can be actively exploited to achieve a security compromise.

In practice, cybersecurity vulnerabilities manifest across multiple layers of the technology stack. At the hardware layer, vulnerabilities may include flaws in processors (e.g., Spectre and Meltdown) that enable side-channel attacks. At the firmware and operating system levels, vulnerabilities may involve privilege escalation opportunities or insecure boot processes. At the application layer, vulnerabilities range from SQL injection to cross-site scripting (XSS) and insecure deserialization. At the network layer, misconfigurations and protocol weaknesses (e.g., legacy support for insecure encryption algorithms) represent enduring sources of risk.

The lifecycle of a vulnerability is itself an intricate subject. It typically begins with the introduction of the flaw during design, development, configuration, or operation. Discovery may occur internally (through testing, auditing, or monitoring) or externally (by security researchers, ethical hackers, or malicious actors). Following discovery, responsible disclosure practices dictate that the vulnerability be reported to the vendor or system owner, patched appropriately, and communicated to users. However, vulnerabilities may also be stockpiled by intelligence agencies, sold on gray markets, or used as part of advanced persistent threats (APTs) before public disclosure or patching occurs.

Zero-day vulnerabilities occupy a particularly menacing place in the cybersecurity landscape. These are flaws unknown to the vendor and therefore unpatched, leaving systems defenseless against exploitation. The discovery and weaponization of zero-days have fueled the rise of sophisticated cyber-espionage campaigns and cyberwarfare activities, underscoring the geopolitical dimension of vulnerability management.

Another essential perspective is the difference between exploitable and non-exploitable vulnerabilities. Not all vulnerabilities are practically exploitable. Some require unrealistic attacker capabilities, privileged internal access, or specific environmental conditions. Assessing exploitability is vital for prioritization: organizations cannot fix every vulnerability immediately and must focus on those most likely to be exploited with significant consequences. Moreover, the exploitation of vulnerabilities does not occur in isolation. Attackers often chain multiple vulnerabilities together to achieve their objectives, leveraging an initial foothold gained through one weakness to escalate privileges, move laterally, and eventually compromise high-value assets. Understanding the potential for vulnerability chaining — and thus modeling vulnerabilities not merely as discrete elements but as interconnected opportunities — is crucial for realistic threat modeling.

In the broader socio-technical system, the presence of vulnerabilities reflects the tension between innovation and security. Software development pressures, market competition, complex supply chains, and user demand for functionality often incentivize speed and feature delivery over comprehensive security validation. Consequently, vulnerabilities are an inevitable byproduct of contemporary cyber technological ecosystems. Acknowledging this inevitability shifts the cybersecurity paradigm from a futile quest for absolute security to a pragmatic focus on resilience, detection, response, and continuous improvement.

Educationally and culturally, fostering a security-conscious mindset among developers, administrators, users, and organizational leaders is paramount to reducing the prevalence and impact of vulnerabilities. Secure software development life cycles (SSDLCs), threat modeling exercises, secure coding standards, and rigorous quality assurance processes serve as indispensable tools in the proactive mitigation of vulnerabilities.

Beyond technical concerns, it is essential to appreciate the ethical dimension of vulnerability research and disclosure. Ethical hackers, often called security researchers, play a vital role in uncovering vulnerabilities that would otherwise remain hidden and exploitable. Coordinated vulnerability disclosure programs, including bug bounty initiatives, have institutionalized pathways for reporting and remediating vulnerabilities responsibly, balancing the public interest with vendor remediation capabilities.

So defining a cybersecurity vulnerability requires more than a static description; it demands a holistic understanding of technological, human, organizational, and adversarial factors. A cybersecurity vulnerability is not merely a technical defect but a dynamic condition embedded within a socio-technical context, subject to discovery, exploitation, mitigation, and evolution. Only through a comprehensive, context-aware approach can organizations hope to navigate the complex landscape of vulnerabilities and build resilient, trustworthy systems.

1.2 Differences Between Vulnerability, Threat, and Risk

In the intricate domain of cybersecurity, the terms "vulnerability," "threat," and "risk" are often deployed interchangeably by the uninitiated, contributing to widespread conceptual confusion. Yet, each term encapsulates a distinct and crucial facet of security discourse. An accurate understanding of these differences is not merely a matter of semantics; it constitutes a prerequisite for effective risk assessment, mitigation planning, and strategic decision-making within organizational and operational security contexts.

A *vulnerability*, as delineated previously, is an inherent weakness, flaw, or deficiency in a system — whether technical, procedural, or human — that could be exploited to compromise security objectives. It represents a potential for harm but does not in itself cause harm. A vulnerability is passive, latent, awaiting activation through the agency of an adversarial force or inadvertent event.

A *threat*, by contrast, is an active agent or circumstance capable of exploiting a vulnerability. It embodies intent, capability, or causality. A threat may originate from malicious actors, natural disasters, technological failures, or even unintended human actions. Threats introduce the dynamic element necessary for vulnerabilities to be realized; without a threat actor or event, a vulnerability remains inert, a theoretical risk factor rather than an operational concern. Risk, finally, arises from the intersection of vulnerability and threat. Risk is the probabilistic expectation of loss or damage resulting from the successful exploitation of a vulnerability by a threat. It encapsulates not only the likelihood of occurrence but also the potential magnitude of impact. Thus, risk serves as the quantifiable and actionable metric guiding security investments, prioritizations, and countermeasures.

To illustrate these distinctions concretely, consider a web application susceptible to SQL injection due to inadequate input validation — a classic example of a vulnerability. A threat would be a cybercriminal equipped with knowledge and tools to identify and exploit SQL injection flaws. The risk materializes in the potential consequences: unauthorized access to sensitive customer databases, leading to data breaches, regulatory penalties, reputational harm, and financial losses.

Understanding the interplay between these three elements necessitates a granular appreciation of their attributes:

• Vulnerability: The Precondition

Vulnerabilities possess several defining characteristics:

- Existence independent of exploitation
- Varied origins
- Potential for discovery and exploitation
- Dynamic exposure

• Threat: The Catalyst

Threats are characterized by several essential dimensions:
- Actor-based or event-based
- Intent and capability
- Persistence and evolution
- Relevance to specific vulnerabilities

• Risk: The Outcome

Risk integrates multiple variables:
- Likelihood
- Impact
- Exposure
- Contextual dependencies

• Interrelationships and Practical Implications

The relationship among vulnerability, threat, and risk is not linear but dialectical. Vulnerabilities invite threats; threats actualize vulnerabilities; risks crystallize from the dynamic tension between vulnerabilities and threats. Mitigating risk thus requires coordinated attention to both vulnerabilities and threats.

• Common Misconceptions and Their Consequences

Failure to distinguish accurately among vulnerability, threat, and risk leads to flawed security strategies:
- Misplaced focus
- Resource misallocation
- Ineffective communication

• The Evolving Landscape

The relationships among vulnerability, threat, and risk are not static. As technology evolves, so do vulnerabilities; as geopolitical tensions rise, so do threats; as business models change, so does risk exposure.

Thus, risk management must be dynamic, continuous, and context-sensitive. Periodic vulnerability assessments, continuous threat intelligence monitoring, and agile risk frameworks are necessary to maintain an accurate, current understanding of organizational risk posture.

1.3 The Role of the ATT&CK Framework

The sequence of attack phases is presented below, along with corresponding examples of vulnerabilities.

ATT&CK Tactic	Example Vulnerabilities
1. Reconnaissance	Information disclosure via public misconfigurations (e.g., open S3 buckets)
2.Resource Development	Compromise of third-party services leveraged for staging attacks
3.Initial Access	Exploitable remote services (e.g., unpatched RDP, VPN flaws)
4.Execution	Remote code execution vulnerabilities in web servers or applications
5.Persistence	Weak authentication mechanisms in startup scripts or services
6.Privilege Escalation	Kernel vulnerabilities (e.g., privilege escalation exploits like Dirty COW)
7.Defense Evasion	Vulnerabilities in endpoint protection evasion (e.g., unprotected script interpreters)
8.Credential Access	Credential exposure through vulnerable password storage or theft via input capture
9.Discovery	Insecure directory listings or unprotected network shares exposing internal topology
10.Lateral Movement	Weak or reused credentials facilitating movement across systems
11.Collection	Applications storing sensitive data unencrypted or without proper access control
12.Command and Control	Outbound connections enabled via firewall misconfigurations
13.Exfiltration	Lack of data loss prevention controls enabling unnoticed data theft
14.Impact	Vulnerabilities enabling ransomware deployment or destructive actions

1.4 Importance of Vulnerability Management

In an era where digital infrastructures underpin nearly every facet of modern civilization — from critical services and economic systems to personal communications and national security — the imperative to safeguard these infrastructures against cyber threats is more pressing than ever. Central to this endeavor is the discipline of vulnerability management. Far from being a mere technical exercise confined to scanning tools and patch deployment, vulnerability management represents a strategic pillar of cybersecurity resilience, governance, and operational assurance.

At its essence, vulnerability management is the continuous, systematic process of identifying, evaluating, prioritizing, remediating, and reporting vulnerabilities within an organization's technology ecosystem. Its goal is to proactively reduce the attack surface available to adversaries, thereby minimizing the likelihood and potential impact of successful exploitation. Yet, the significance of vulnerability management extends beyond simple preventative maintenance; it embodies a philosophy of risk-based, adaptive security aligned with dynamic threat landscapes and evolving organizational priorities.

Vulnerability management is not merely a technical checklist or regulatory checkbox; it is a dynamic, strategic discipline essential to safeguarding organizational assets, operations, and reputations in a hostile digital environment. As the threat landscape evolves, driven by technological innovation, geopolitical dynamics, and adversarial ingenuity, the importance of mature, risk-based, adaptive vulnerability management will only intensify.

Organizations that embrace vulnerability management as a strategic imperative — investing in people, processes, technologies, and cultural transformation — will be better positioned to navigate the perils of cyberspace, seizing opportunities for growth and innovation while protecting what matters most.

1.5 Principal Frameworks and Classification Sources

1.5.1 MITRE ATT&CK

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework represents a monumental shift in how cybersecurity practitioners conceptualize adversary behavior and system vulnerabilities. Rather than focusing solely on vulnerabilities as static technical flaws, ATT&CK maps adversarial behavior in dynamic, operational terms. Developed by the MITRE Corporation, a nonprofit organization with deep roots in research for the U.S. government, ATT&CK was introduced publicly in 2015. It is structured around a series of matrices, most notably the Enterprise Matrix, which categorizes adversarial actions across 14 tactical stages — from initial reconnaissance to ultimate impact. Each tactic encompasses multiple techniques, and many techniques are further broken down into sub-techniques, reflecting the nuanced realities of cyberattacks in the wild.

ATT&CK's approach is uniquely valuable for vulnerability management because it highlights how vulnerabilities are operationalized within broader attack strategies. A vulnerability in remote desktop services, for instance, may directly enable the 'Initial Access' tactic via techniques like 'Exploit Public-Facing Application' or 'Valid Accounts.'

One of ATT&CK's profound contributions is its grounding in real-world adversary behavior. Techniques are not hypothetical but drawn from documented threat actor campaigns. Furthermore, ATT&CK offers rich contextual data, including mappings to specific malware, adversary groups, and recommended mitigations and detections.

Organizations leverage ATT&CK to perform gap analyses of their defenses, simulate adversary behavior in penetration tests and red teaming exercises, prioritize patches based on adversary tendencies, and enrich threat intelligence operations. Its adoption by security operations centers (SOCs), incident response teams, and cyber threat intelligence (CTI) analysts has been transformative. What is more, ATT&CK's public accessibility and continual evolution — incorporating community feedback and new threat research — ensure its relevance in an ever-