Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya
CS559: L21 Pen Testing

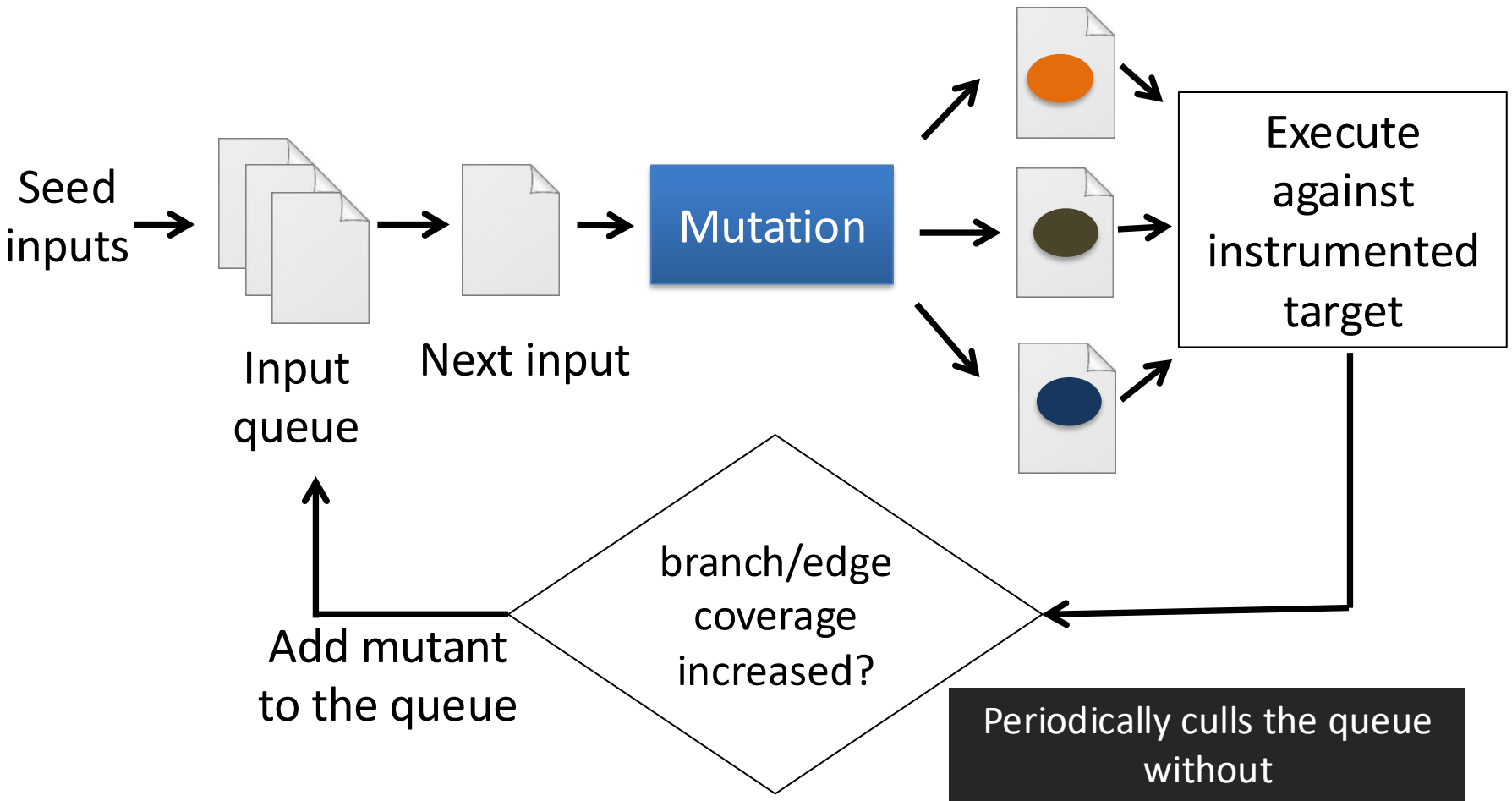


CSU Cybersecurity Center
Computer Science Dept

Coverage-guided gray-box fuzzing

- Special type of mutation-based fuzzing
  - Run mutated inputs on instrumented program and measure code coverage
  - Search for mutants that result in coverage increase
  - Often use genetic algorithms, i.e., try random mutations on test corpus and only add mutants to the corpus if coverage increases
  - Examples: AFL, libfuzzer

American Fuzzy Lop (AFL)



Colorado State University

AI Fuzzing vs. Traditional Fuzzing

Capability	Traditional Fuzzing	AI-Powered Fuzzing
Harness Engineering	Manual: Humans must write the complex code ("fuzz targets") to feed input into an API.	Automated: AI automatically generates syntactically correct, structure-aware fuzz targets at massive scale.
Input Structure (The Seed Pool)	Stochastic / Random: Mutates inputs via random bit-flipping. If a program requires a strict file format the fuzzer gets blocked.	Semantic & Intelligent: AI understands code logic and generates complex, syntax-compliant inputs that bypass early input-validation checks.
Code Coverage	Shallow Depth: Fails to reach hidden or deeply nested logic blocks.	Deep Penetration: Achieves drastically higher code coverage. Google's AI-fuzzing frameworks successfully forced testing tools into obscure code paths across 272 projects that human-written setups never reached.
Target Application	Limited to Binaries: Primarily constrained to compiled code, memory limits, and command-line inputs.	Expands to Natural Language: Extends to testing modern AI models. AI fuzzers can intelligently mutate text prompts to systematically find "jailbreaks" and safety guardrail bypasses.

How AI Accelerates Overall Vulnerability Discovery

- Traditional vulnerability discovery relies on human security researchers manually inspecting source code, reverse-engineering binaries, or setting up static application security testing (SAST) tools that flag thousands of false positives.
- AI speeds this process up.
  - **Autonomous Setup & Orchestration**: AI agents can analyze an entire software library, instantly map out its public APIs, configure build environments, and write the custom testing harnesses required saving hundreds of hours.
  - **Contextual Triaging**: When a security flaw found, AI models can instantly analyze the application's active state, deduce exactly what type of bug it is (e.g., a buffer overflow vs. a use-after-free error), and trace the data flow to prove if it is exploitable.
  - **Closing the Loop**: Advanced platforms create autonomous pipelines. Google's CodeMender, for instance, links AI discovery tools to an LLM that autonomously drafts, tests, and upstream merges a security fix directly back into the codebase

Tool Pipeline

These Google tools function as a unified pipeline:

- **OSS-Fuzz** continuously tests the codebase and generates a crash report.
- **Big Sleep** analyzes the crash context to trace exactly how a malicious actor could exploit it.
- **CodeMender** automatically uses that data, creates a patch, validates that it doesn't break the application, and pushes a pull request directly to the developers.

AI-driven remediation

Patching Phase	Traditional / Without AI	Autonomous / With AI
Typical Enterprise Cycle	30 to 90 days (Governance SLAs typically give 30 days for critical, 60 for high)	6 to 13 days (Autonomous endpoint patching tools)
Average Real-World MTTP	43 days (up from 32 days in 2024 due to increased complexity)	Under 3 days (When integrating AI scanners with virtual patching/WAAP solutions)
Testing & Verification	8 to 14 days of traditional siloed testing	Automated validation and immediate deployment orchestration

Defensive asymmetry

AI has broken traditional, patch-centric vulnerability management.

- **Centralized Bottlenecks: The National Vulnerability Database (NVD) Crisis** NVD, has been overwhelmed by record-breaking CVE growth driven heavily by AI-assisted submissions. Of the more than 53,000 CVEs published by late 2026, nearly 79% sit in an "Awaiting Analysis" backlog. Roughly 80% of new CVEs are now labeled "Not Scheduled.
- **The Open-Source & Maintainer Chokepoint** Anthropic's Project Glasswing utilized AI to surface 26,153 vulnerabilities. Out of more than 2,000 officially disclosed to maintainers, fewer than 1% have actually been patched.
- **Enterprise Triage Overwhelm** :
  - **Signal vs. Noise:** Poorly implemented AI code scanners routinely drop massive lists of unvalidated flaws into development backlogs, sometimes yielding true-positive rates below 7%.
  - **Fixing vs. Breaking:** more than 53% of AI-generated patches either failed to fix the core vulnerability, broke application logic entirely, or introduced brand-new security flaws.

Quantitative Security

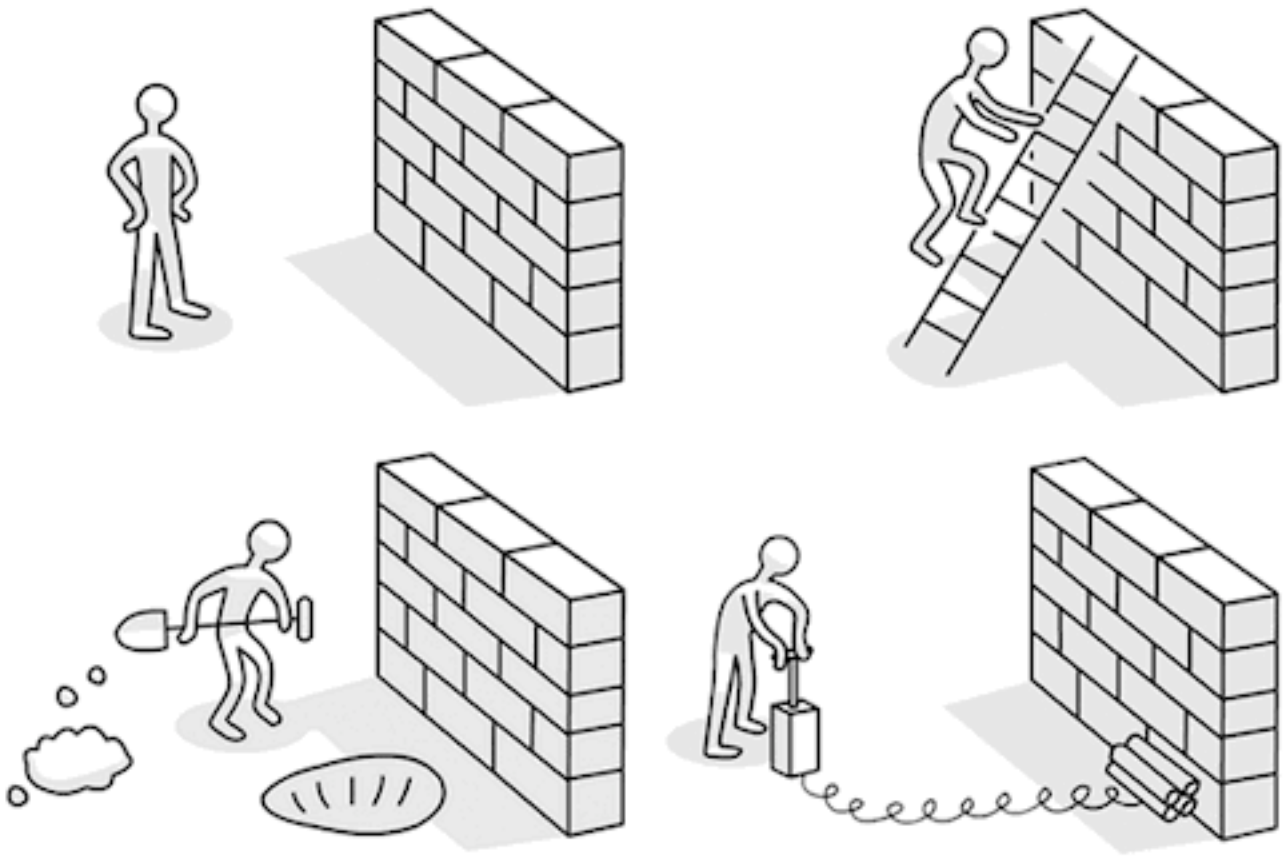
Colorado State University
Yashwant K Malaiya

CS 559
Penetration Testing



CSU Cybersecurity Center
Computer Science Dept

Penetration Testing



https://www.cobalt.io/blog/how-to-choose-a-pentest-service

Colorado State University

Penetration Testing

How to get into a system and steal stuff

- Not legal in general
- Completely legal if you are hired and authorized to do Pen Testing. Very valuable service.
- Involves all kinds of bad/fun stuff.
- A **penetration test**, or a **pen test**, is a simulated cyber attack against a computer system (or enterprise) to check for exploitable vulnerabilities.

Teaching How to Pick a Pocket or Two



- Fagin in Charles Dicken‘s Oliver Twist (1838)
- https://www.youtube.com/watch?v=2YVAmZBGdXw Fifth Av Theater

- A remote area in Jharkhand's Maoist-hit **Jamtara** district, a man runs a coaching centre where he teaches his pupils trader tricks of online fraud

Quantitative Security

Colorado State University

Yashwant K Malaiya

CS 559

Penetration Testing



CSU Cybersecurity Center
Computer Science Dept

What is Penetration Testing?

- Definition: A penetration test is a method of evaluating the security of a computer system and/or network by simulating an attack from a malicious source
  - malicious source: also known as a Black Hat Hacker
- A Pen Tester vs a Hacker
  - Prior approval
    - Pen Tester's have prior approval from Senior Management.
    - Hackers need no approval.
  - Technical Skills and Tools
    - A Pen Tester's uses his technical skills & tools to identify weaknesses that needs fixing.
    - A hacker wants to exploit weaknesses for profit or satisfaction
  - Social Engineering Skills
    - Pen Tester's social engineering penetration attempts are there to raise awareness
    - Hackers social engineering attacks are to steal/damage data

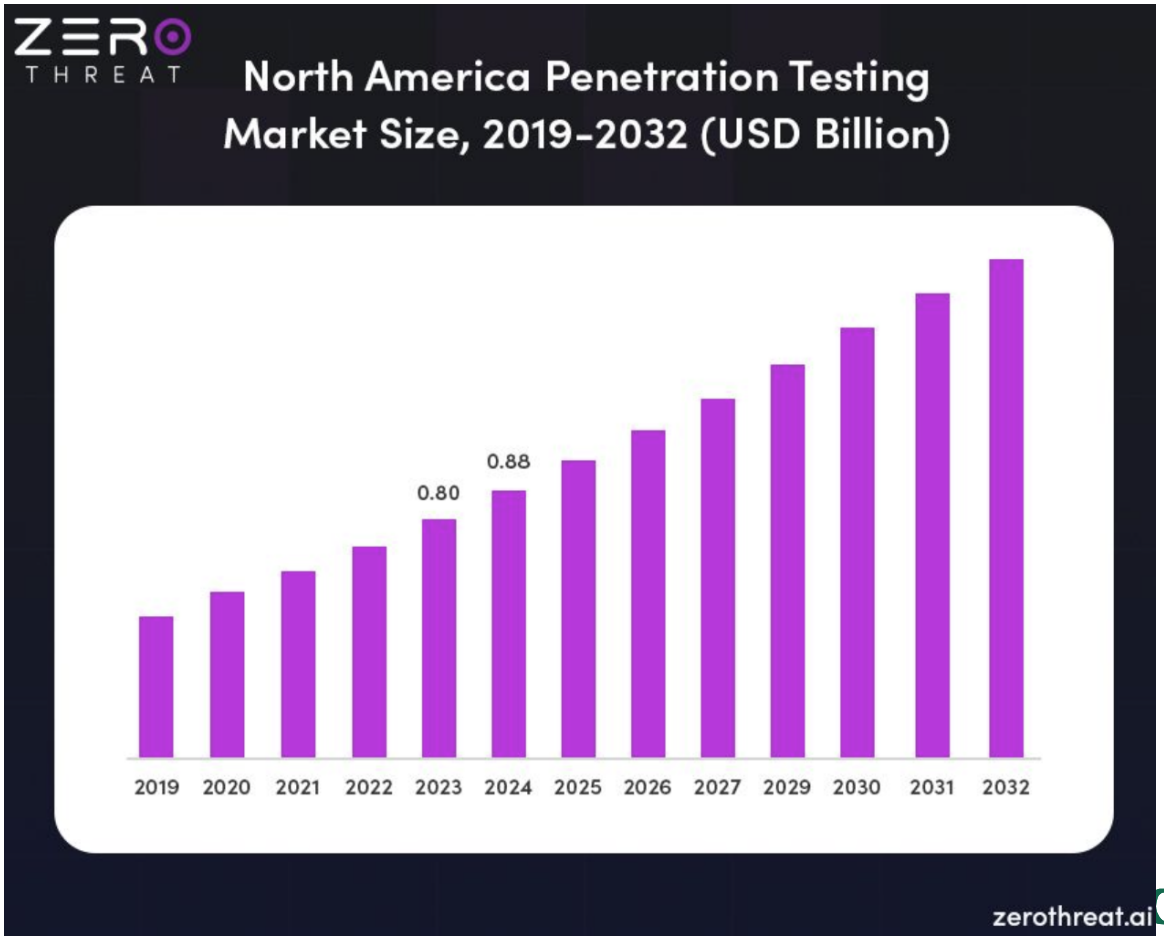
Ack: NASA-Ames, 2010

Where are details?

- We will only look at higher level considerations.
- There are numerous interesting details that will take many hours of discussions/demonstrations. It can take a year to become an expert.
- Many powerful tools are in public domain and can be downloaded and installed.
- For example, you can run Kali Linux in a virtual machine.
  - It has a number of powerful tools included: Vulnerability analysis, Wireless attacks, Exploitation tools, Password attacks, Sniffing and Spoofing etc.
- Caution: Much of the information available has been created by those who wish to sell their services.

Market

- The market is projected to grow from USD 2.74 billion in 2025 and reach USD 6.25 billion by 2032, exhibiting a CAGR of 12.5% during the forecast period.
- [The State of Penetration Testing 2025: What the Numbers Reveal]



Penetration Testing vs Vulnerability Assessment

- **Vulnerability Assessment**: *process of identifying, evaluating, and classifying security vulnerabilities based on the risk they present*
  - Typically conducted by in-house staff using authenticated credentials; does not require a high skill level.
  - Planned internally by the organization. Known timing.
  - Unreliable at times and high rate of false positives. *(that is claim)*
  - Vulnerability assessment invites debate among System Admins.
  - Produces a report with mitigation guidelines and action items.

- **Penetration Testing**: *(pen testing or ethical hacking), is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit*
  - Generally an independent outside service; requires a great deal of skill
  - Focused in scope and may include targeted attempts to exploit specific vectors (Both IT and Physical)
  - Unpredictable for the internal people.
  - Highly accurate and reliable. *(that is claim)*
  - Penetration Testing = Proof of Concept against vulnerabilities.
  - Produces a binary result: Exploitable holes identified and proven.

Ack: NASA-Ames, Penetration Testing and Vulnerability Assessment, 2010

Scope of Penetration Testing

- Targeted Reconnaissance and penetration
  - Targeted exploitation of vulnerabilities.
  - Network/Firewall Vulnerability Testing
  - Web Application Vulnerability Testing
  - Cloud Computing Penetration Testing
  - Mobile app Penetration Testing
- Social Engineering (Phishing, pharming, spear-phishing)
  - Can you tell me what my password is?
- Physical facilities audit (Unlocked terminals, unsecure building)
  - Sorry, I forgot my badge...
- Wireless Access
  - Detection of rogue or weakly encrypted AP's. (TKMaxx breach etc)
- Dumpster Diving
  - I've found someone's Tax forms with SSN.

Internal vs External Penetration Testing

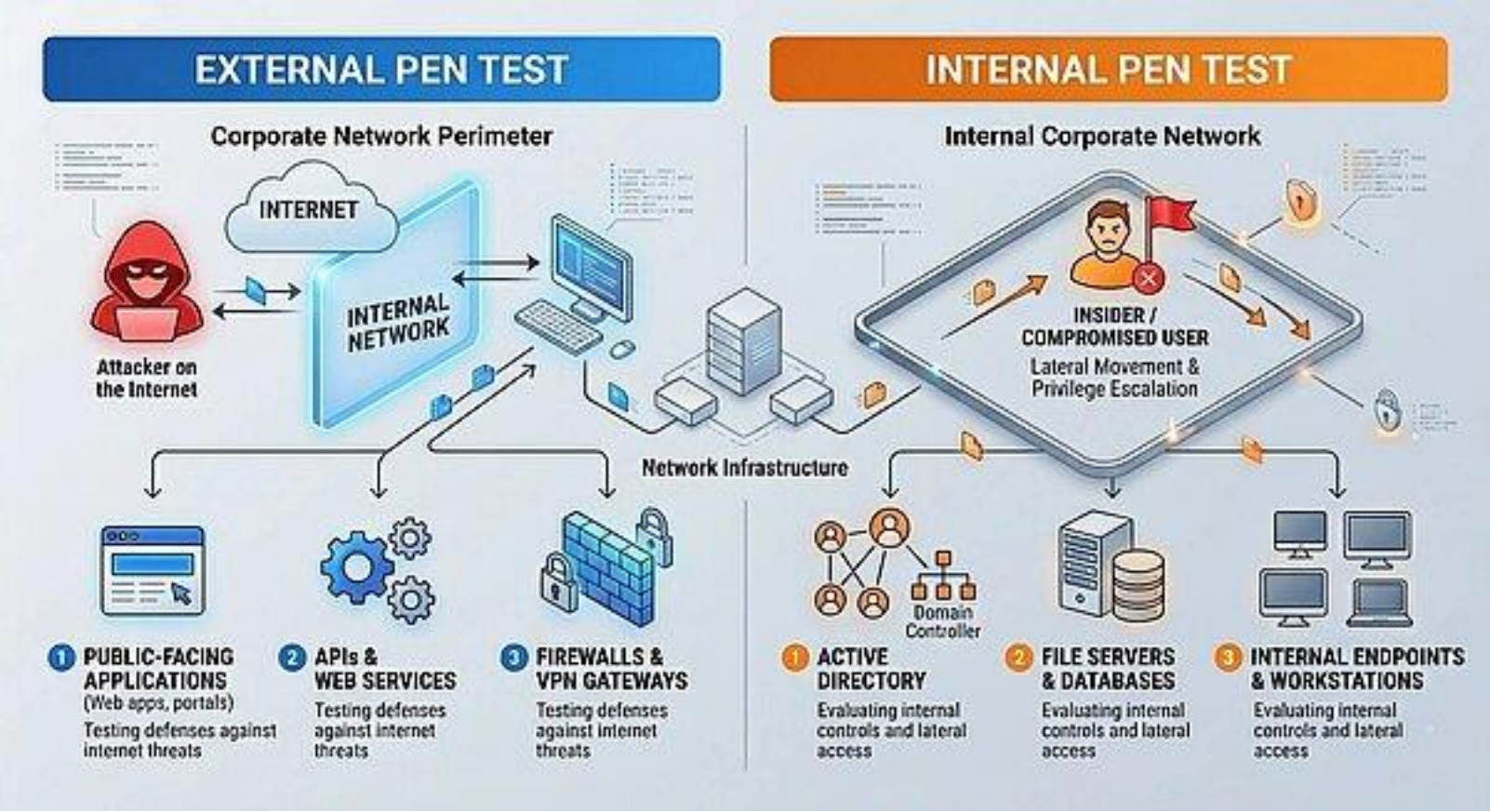
Factor	External Penetration Test	Internal Penetration Test
Attack Vector	Outside the organization	Inside the organization
Simulates	External hackers / APTs	Insiders / post-breach attackers
Targets	Internet-facing assets	Internal systems & data
Primary Risk	Perimeter vulnerabilities	Lateral movement & privilege escalation
Compliance Use	PCI-DSS, ISO 27001, SOC 2	HIPPA, GDPR, ISO 27001
Frequency	Annually or after major changes	Annually or after incidents
Complexity	Moderate to High	High

https://www.pitsolutions.com/blog/internal-vs-external-penetration-testing-key-differences-strategy

Standards: PCI-DSS (Credit cards), SOC 2 (Accountants), ISO 27001 (International)
HIPPA (healthcare), GDPR (European), ISO 27001 (International)

Colorado State University

Pen Testing: Internal vs External



https://www.pitsolutions.com/blog/internal-vs-external-penetration-testing-key-differences-strategy

Colorado State University

Pen Testing Metrics

Program Level Metrics

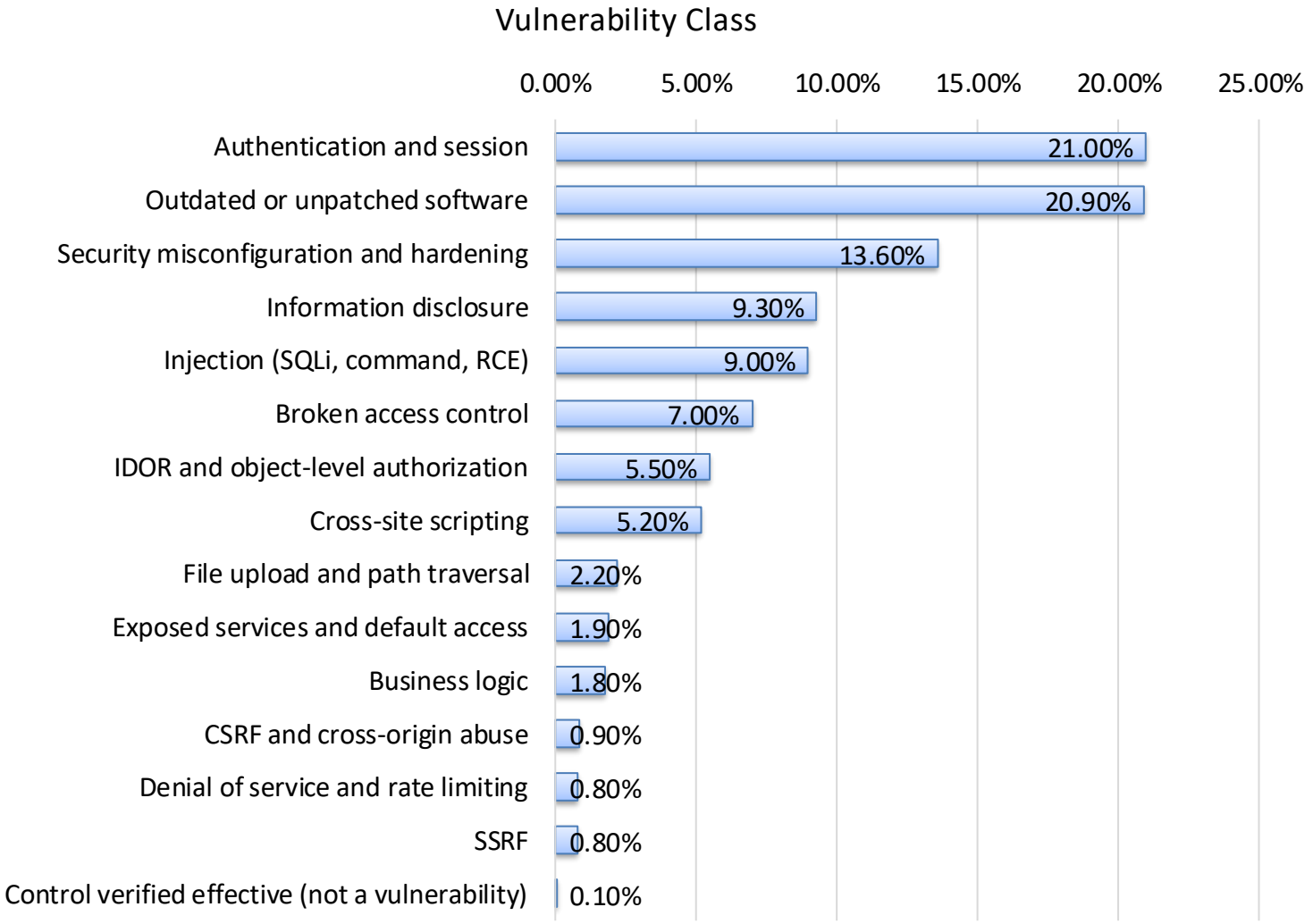
- Application Portfolio Coverage
  - An organization should apply security controls in a risk-based manner across its entire application portfolio.
  - Coverage = # of applications tested/ total # of applications
    - Applications include web, mobile, APIs
- Test Frequency & Time to Fix
  - a penetration test on critical applications two to four times a years, or upon major changes.
  - Critical findings should be fixed as soon as possible.

Engagement Level Metrics

- Vulnerability Types
  - How real-world vulnerabilities map to recognized vulnerability categories
  - Their criticality
  - Applying fixes

Pen Test Metrics 2018

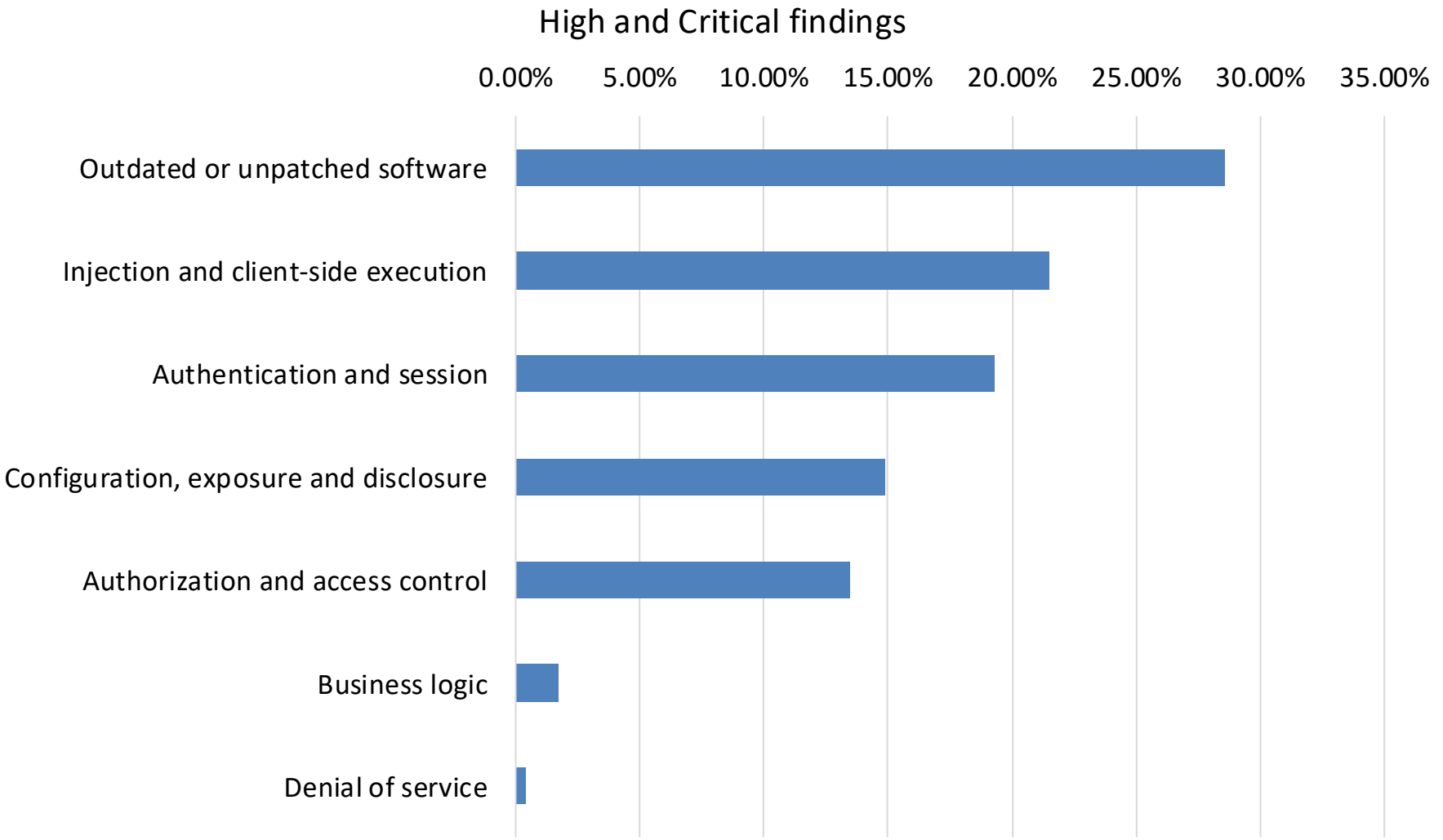
Common Pentest findings in 2026



https://www.stingrai.io/blog/state-of-penetration-testing-2026

Colorado State University

High and Critical Findings



Colorado State University

A wave of disruptions at grocery stores

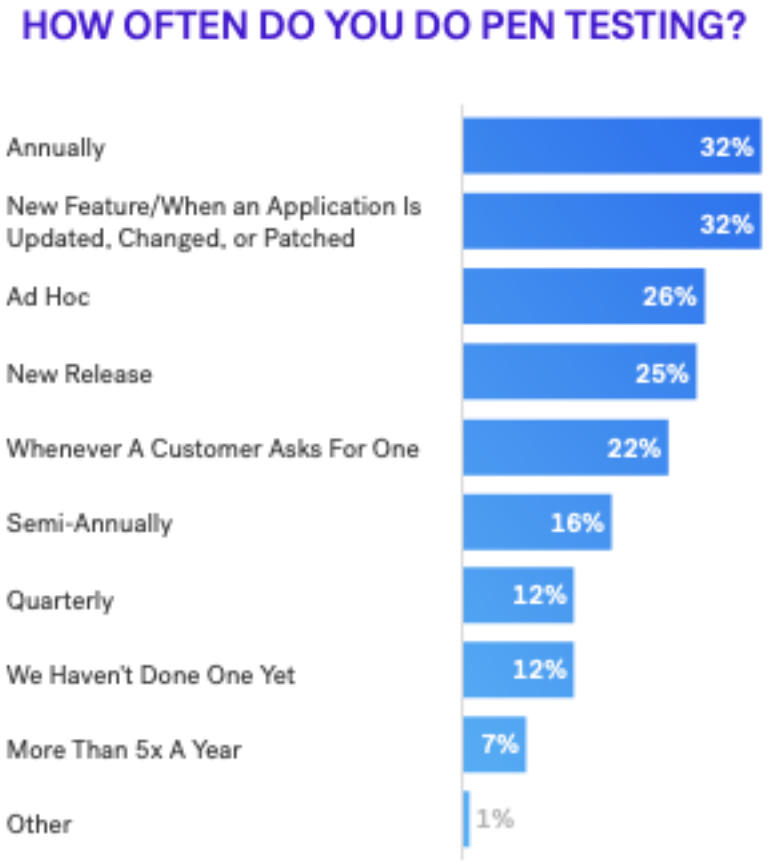
Are Freezers Being Hacked? Europe and the U.S. Military Investigate? Nov 2, 2026

- Last month, freezers malfunctioned at hundreds of grocery stores in France in what officials called a cyberattack. On Monday, retailers in at least seven more Europe.
- The attack in France last month targeted systems made by three manufacturers whose units were remotely controlled, the national cybersecurity agency said at the time. Danfoss, one of the manufacturers, said that most of the affected units were older and **did not have software updates that many manufacturers now use to secure their systems**.



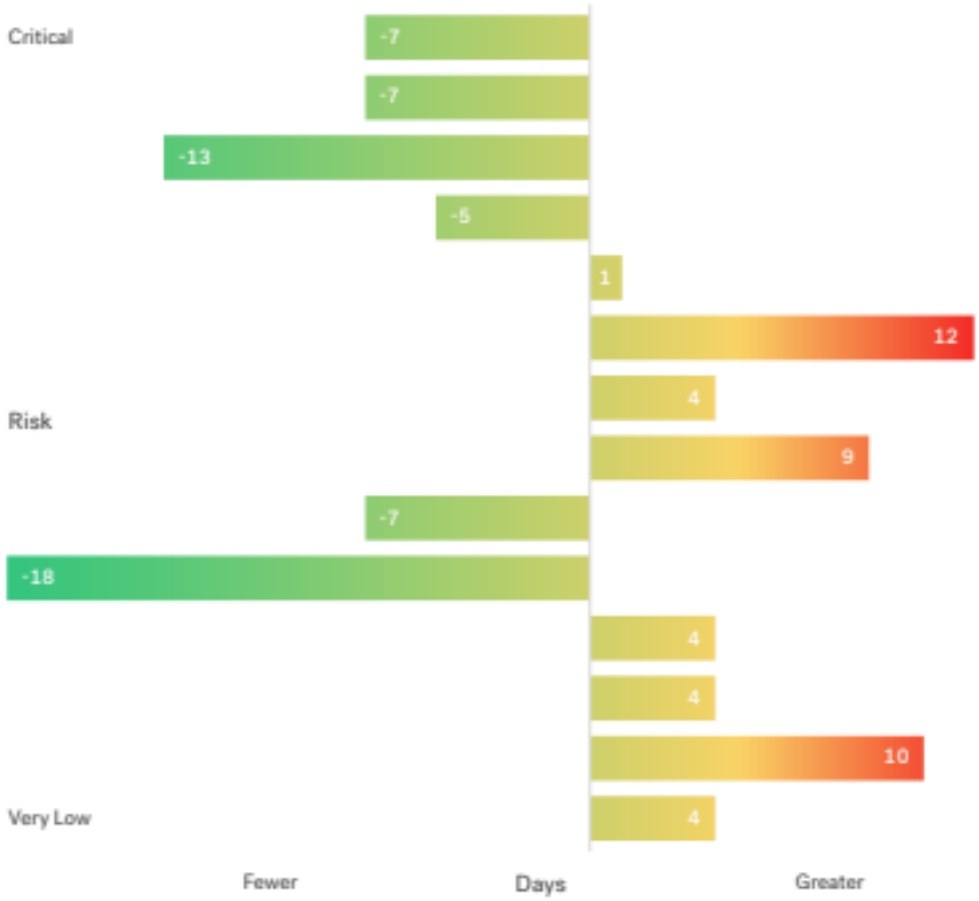
Colorado State University

HOW OFTEN DO YOU DO PEN TESTING?



Colorado State University

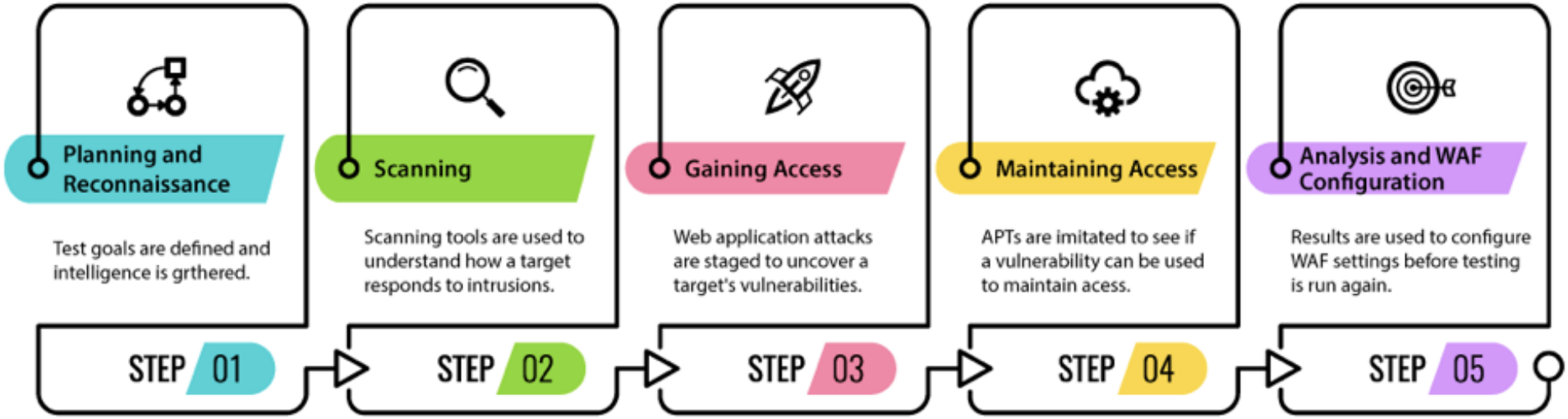
RELATIVE DAYS FOR ORG TO RESOLVE RISK



Data from Cobalt's pen testing as a service platform, based on 250+ pen tests conducted in 2017

Colorado State University

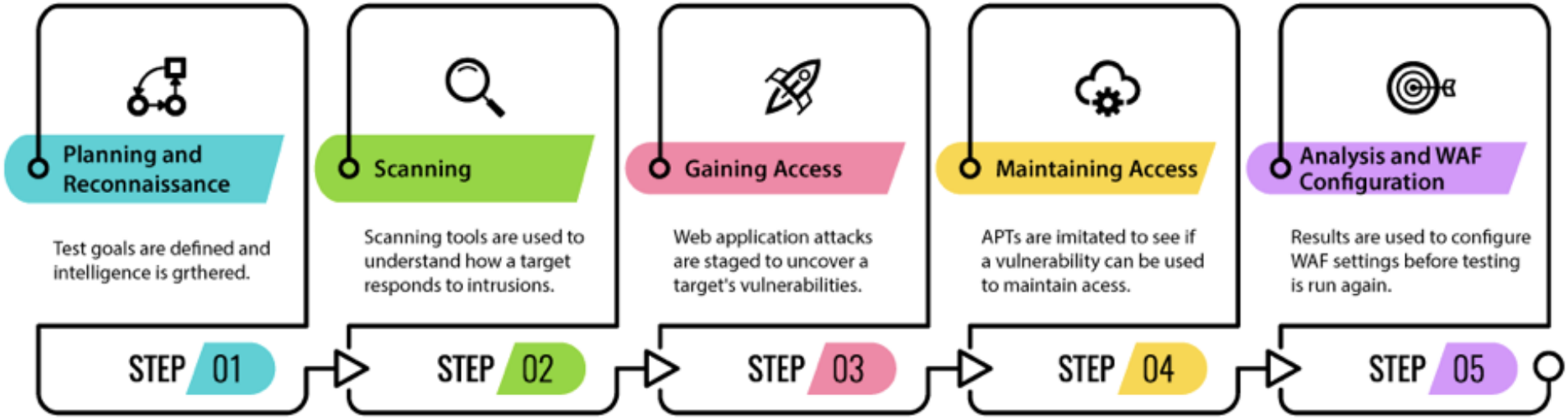
Pen Testing Stages



1. Planning and reconnaissance
   - Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
   - Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.
2. Scanning
   - Network scanning and topology tracing, id OS and applications, Port scanning to find open ports and services, find net addresses of live hosts, firewalls, routers, etc. vulnerability scans to id potential vulnerabilities.
3. Gaining access:
   - This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

Sources: Bhamre, Imperva

Pen Testing Stages



4. Maintaining access: See if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access.

- The idea is to imitate advanced persistent threats (APTs), which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis and remediation: The results of the penetration test are then compiled into a report with

- Specific vulnerabilities that were exploited, Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected
- This information is analyzed help configure an enterprise's WAF (web protection firewall) settings and security solutions to patch vulnerabilities and protect against future attacks.

Sources: 1, 2

Pen Testing Tools

- 1. The Network Mapper (also known as "NMAP", competitor Nessus)
  - NMAP can take the raw data packets which have just been created and use that to determine the following:
    - What hosts are available on a particular network trunk or segment
    - The information about the services which are being provided by these hosts
    - What operating system is being used (this is also known in technical terms as "Fingerprinting")
    - The versions and the types of data packet filters/firewalls are being used by any particular host
- 2. Metasploit: a package of different Pen Testing tools
  - with a built-in network sniffer, and various access points from which to mount and coordinate various kinds of Cyber based attacks.
  - This is accomplished via a quick, four step processes:
    - Determine which prepacked exploit should be used (or customize your own)
    - Configure this particular exploit with both the remote port number and IP address
    - Ascertain which payload should be used
    - Configure the payload with both the local port number and IP address
    - Launch the exploit at the intended target
  - This tool also comes with a "Meterpreter" which displays the results after an exploit has occurred

https://resources.infosecinstitute.com/category/certifications-training/pentesting-certifications/top-pentesting-tools/#gref

Pen Testing Tools

- 3. Wireshark: an actual network protocol and data packet analyzer
  - live information and data can be collected from: IEEE 802.11, Bluetooth, SSL/TLS, …WEP, ..Any Ethernet based connections
  - useful in analyzing the Security risks when information and data are posted to forms on Web based applications. These threats include data parameter pollution, SQL injection attacks, and memory buffer overflows.
- 4. The Web Application Attack and Audit Framework (also known as the "W3AF")
  - can root out threats such as:
    - User-Agent Faking
    - Custom Headers to Requests
    - DNS Cache Poisoning (this is also known as "DNS Spoofing," and it occurs when the DNS Name Servers return an incorrect IP address. As a result, the legitimate network traffic is diverted to the Cyber attacker's computer)

Pen Testing Tools

- 5. John the Ripper: primarily to launch Dictionary Attacks
  - Pen Test password databases which are both online and offline.
- 6. Kali Linux: Debian-derived Linux distribution designed for digital forensics and penetration testing
  - Numerous preinstalled penetration-testing programs, including Armitage (a graphical cyber attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), John the Ripper password cracker, Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners

Vulnerability Scanners

- Study at Swedish Defense Research Agency
- Environment was composed of 20 physical servers running a total of 28 virtual machines, four VLAN segments; Windows XP SP2, Debian 5.0 and Windows Server 2003 SP1; HTTP, HTTPS, SMTP, FTP, Streaming Media Server, RDP, SSH, SMB and VNC
- Unauthenticated (without logging in) and authenticated (logged in) scans

Table 4. Overview of identified vulnerabilities.

Scanner	Unauthenticated scan				Authenticated scan			
	High	Medium	Low	Potential	High	Medium	Low	Potential
AVDS	46	140	306		291	990	393	
McAfee VM	143	169	64		2028	2033	126	
Nessus	145	82	889		2221	468	1256	
NeXpose	180	391	106		1073	969	126	
Patchlink scan	1	4	15		814	328	313	
QualysGuard	73	125	151	284	753	1891	342	313
SAINT	81	60		223	114	65		257

Vulnerability Scanners

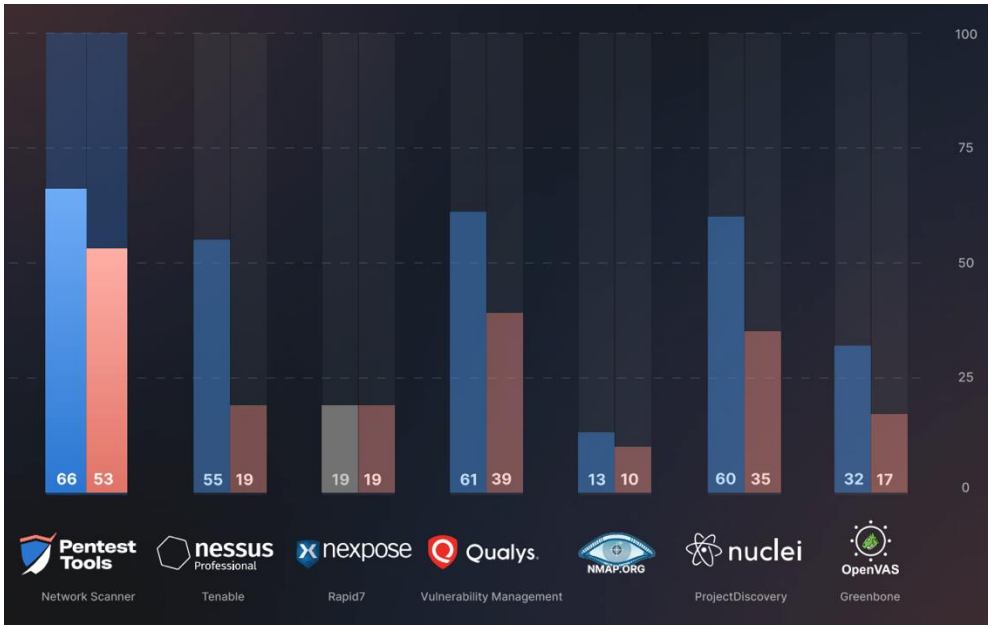
Tool	Detection %	False alarm (%)
AVDS	34	0
McAfee	36	3
Nessus	43	5
NeXpose	43	5
Patchlink scan	36	6
QualysGuard	55	10
SAINT	43	13

Hannes Holm and Teodor Sommestad and Jonas Almroth and Mats Persson, A quantitative evaluation of vulnerability scanning, Inf. Manag. Comput. Secur., V 19, No. 4, 231—247, 2011

Pen Testing Costs (examples)

- From a vender, includes Pre-Test Discovery to define goals and a detailed Final Report
  - Up to 1 External IP starting at $1,195
  - Vulnerability Scan and Pen Test bundles as low as $1,495
  - Web Application Pen Tests starting at $2,500.
- From RSI
  - can cost $4,000-$100,000. On average, a high quality, professional pen test can cost from $10,000-$30,000, depending on
    - Organization size, complexity, scope, remediation
    - Methodology, Experience
    - External (common)/Internal Testing
- Pen testing industry: $218 billion/year, av salary 120K/y

Benchmark results against all Vulhub vulnerabilities



https://pentest-tools.com/benchmarks/network-vulnerability-scanners-benchmark-2024.pdf

Detection availability = count of the detection existence/total number of vulnerabilities

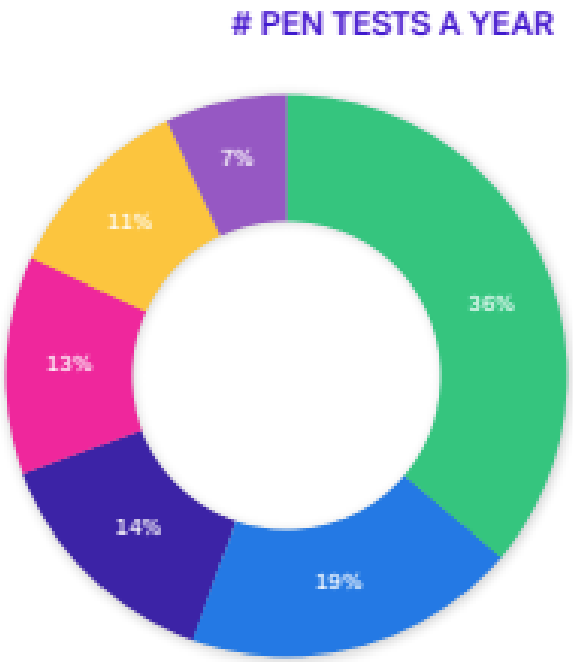
Detection accuracy = count of the vulnerabilities detected/total number of vulnerabilities

How Often Should we Perform a Penetration Test?

- Regularly, at least once a year
  - Many regulations, such as PCI DSS, SOX, and HIPAA require an annual penetration test from a third party.
- Other times when
  - new network infrastructure or applications added
  - significant upgrades /modifications to applications or infrastructure
  - offices in new locations established
  - Security patches applied
  - end-user policies modified
- Example policy:
  - critical findings customer facing applications be fixed within 48 hours, high severity findings within 10 days, medium severity within 30 days, and low severity within 90 days.
- Typical value
  - 2016 av time to fix critical pen test findings = 17.6 days.
  - 2016 distribution: critical 9%, High 6%, Med 14%, Low 72%

How many pen tests do you do a year?

a. In 2017, cobalt.io collected data from 75 survey respondents in security, management, operations, DevOps, product, and developer roles





b. WHAT IS MOST CHALLENGING ABOUT PEN TESTING APPLICATIONS?

Source of data

Colorado State University

PCI Data Security Standard (PCI DSS v3)

Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3 Penetration Testing Guidance (pdf)

- **Penetration Testing Components**: Understanding of the different components that make up a penetration test and how this differs from a vulnerability scan including scope, application and network layer testing, network segmentation checks, and social engineering
- **Qualifications of a Penetration Tester**: Determining the qualifications of a penetration tester, whether internal or external, through their past experience (>1y) and certifications.
- **Penetration Testing Methodologies**: Detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement.
- **Penetration Testing Reporting Guidelines**: Guidance for developing a comprehensive penetration test report that includes the necessary information to document the test as well as a checklist that can be used by the organization or the assessor to verify whether the necessary content is included.

For further information

- **The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy**, Patrick Engebretson, Syngress, 2nd edition (August 15, 2013)
- **Learn Kali Linux 2019: Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark** Paperback, Glen D. Singh, Packt Publishing (November 14, 2019)
- **Full Ethical Hacking Course - Network Penetration Testing for Beginners** (2019), 15 hours Video
- A sample Penetration Test Report.

AI in PenTesting

AI is included in phases of the offensive security lifecycle, shifting the industry toward **continuous pentesting** rather than static, once-a-year compliance audits.

- **Autonomous Reconnaissance & Attack Path Modeling**: AI agents process massive datasets to map out an enterprise's external and internal attack surfaces. Instead of following a single, linear attack path, AI can use lateral movement and model complex, multi-vector scenarios.
- **Vulnerability Triage & Prioritization:** Tools like **Pentera** can identify the vulnerabilities that pose the highest actual business risk.
- **Context-Aware Exploit Generation:** LLMs tools like **PentestGPT** and specialized agents can analyze specific code blocks or network responses to generate customized payloads or bypass signature-based detection systems.
- **Advanced Social Engineering:** Generative AI is utilized to craft highly context-specific phishing campaigns that mimic an organization's internal communication style, testing human defenses at an unprecedented scale.
- **Automated Documentation & Reporting:** AI bridges the gap between technical findings and business risk. It automates the tedious process of writing comprehensive technical summaries and code-specific remediation guidance for developers.

How Effective is AI in PenTesting?

Metric / Aspect	Performance & Impact
Speed & Efficiency	Tools like **PentestGPT** have been shown to boost pentesting sub-task workflow efficiency by over 200%. AI-driven attacks can chain low-severity bugs into critical compromises in under an hour.
Vulnerability Detection	Purpose-built AI agents can outperform the median human pentester at standard OWASP Top 10 web vulnerabilities. In a real-world enterprise test, the academic agent **ARTEMIS** beat 9 out of 10 human cybersecurity professionals at scanning and mapping.
Success Rates	Specialized LLM frameworks like RapidPen show up to a 60% success rate in autonomously gaining initial shell access on target systems at a very low cost.
Primary Weakness	AI fundamentally struggles with multi-step authorization flaws, complex application logic, and creative attack chains that require a deep, understanding of how an application is supposed to behave.
The "Hallucination" Problem	AI models frequently produce confident, fabricated findings. Effective security harnesses must enforce an "evidence-only" rule, blocking a finding until the agent provides reproducible proof.

How Popular is AI PenTesting?

- The global penetration testing market is projected to skyrocket from **$1.92 billion in 2023 to nearly $7 billion by 2032.**
- **Adoption Rates:** Roughly **30% of cybersecurity teams have actively integrated AI** into their testing workflows, while an additional **42% are currently evaluating** how to deploy it securely.

Pentesting Method	Average Cost Range	Pricing Basis	Retesting & Hidden Costs
Traditional Manual Pentest	$10,000 – $50,000 (Boutique/Mid-market) $100,000+ (Big 4 Consultancies)	Per engagement based on target scope (e.g., number of IPs, API endpoints, or user roles).	High. Verification scans to check your fixes usually cost an extra $5,000 – $15,000 per retest.
Agentic / Pure AI Pentest	$4,000 – $8,000 (Per application model) $20,000 / year (Continuous enterprise network monitoring)	Subscription or Per-Asset. Unlocks year-round testing capabilities instead of point-in-time snapshots.	Zero. The software-driven model automatically tests and verifies your remediation deployments at no added cost.
AI-Assisted Human Service	$20,000 – $100,000+ (PTaaS - Penetration Testing as a Service)	Annual Retainer / Credits. Humans validate what the automated systems discover.	Included. Retesting and validation are baked directly into the active annual service contract.

Performance Profiles

Tool / Platform	False Positive	False Negative	
Pentera 2015	Near-Zero (<1%)	Low-to-Medium	**Market Leader (Enterprise)**. One of the most mature platforms with substantial Fortune 500 penetration.
Horizon3.ai (NodeZero) 2019	Near-Zero (<1%)	Low-to-Medium	**Strong Mid-Market / Enterprise Contender**. Rapidly growing footprint across corporate internal infrastructures.
XBOW 2023	Near-Zero (<1%)	Medium	**Emerging Pure-Play Leader**. Widely recognized as a highly advanced autonomous web application agent framework.
Aikido Security 2022	Medium (Variable)	Low	**Top Developer-First Platform**. High adoption rate among fast-moving startups and product teams.
PentestGPT 2023	High	High (Without human validation)	**Community Standard**. The go-to open-source option for individual red-teamers and independent researchers.

Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
Attacks



CSU Cybersecurity Center
Computer Science Dept

Attacks

- Assets and threats
- Attack types
- Attack surfaces
- Attack trees

Based on Computer Security Principles and Practice, Fourth Edition, William Stallings and Lawrie Brown

Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Table 1.3

Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

Attack Surfaces

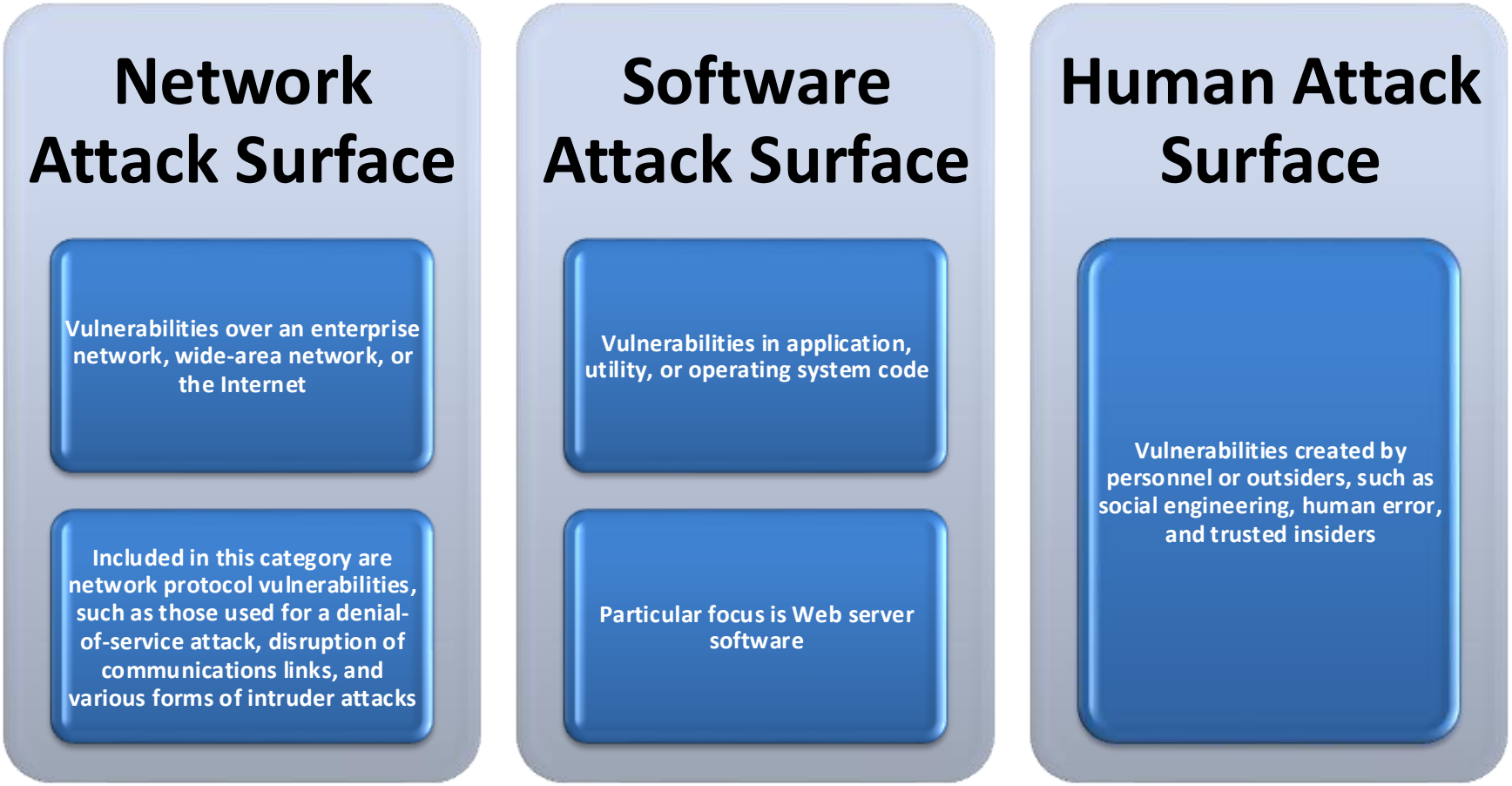
Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Colorado State University

Attack Surface Categories



Colorado State University