Embedding the Attacker's Perspective

Evan Anderson

About Speaker

Evan Anderson

Founding Team & Principal Technologist, Randori.

More than 15 years of experience in red teaming, vulnerability research, exploit development and is a founding member of the NCCDC Red Team. Prior to co-founding Randori, he worked at Kyrus Technologies supporting commercial and federal projects.

Attacker POV Compromise is inevitable.

FACT

Attackers take the time to **KNOW** the system.

FACT

Attackers have **EXPERTISE** organizations don't.

Randori POV

Compromise is inevitable,
Breaches are NOT.

20k+

Software vulnerabilities reported in 2021.

4k+

CVE’s have a High or Critical severity.

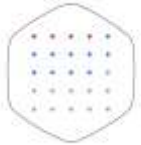
Through 2026, **non patchable attack surfaces** will grow from less than 10% to **more than half** of the enterprise’s total exposure, reducing the impact of automated remediation practices.

Gartner

Randori
an IBM Company

Point of View

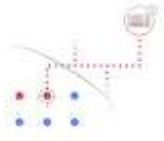
Defenders See Vulnerabilities



- ✓ Firehose
- ✓ Snapshot in Time
- ✓ Overly Specific
- ✓ Presumes knowledge
- ✓ Lacks Context

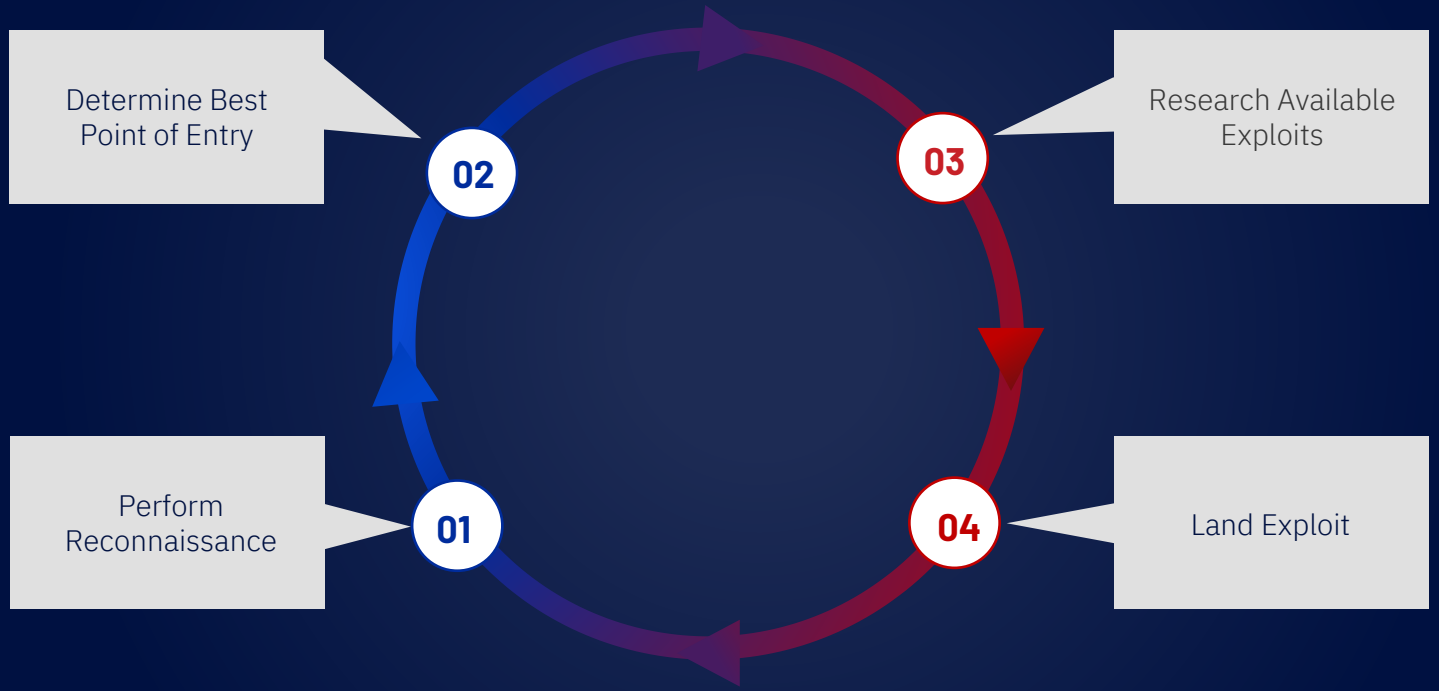
VS

Attackers See Targets



- ✓ Attackable
- ✓ Interconnected
- ✓ Dynamic
- ✓ Unique

Steps in a Successful Breach

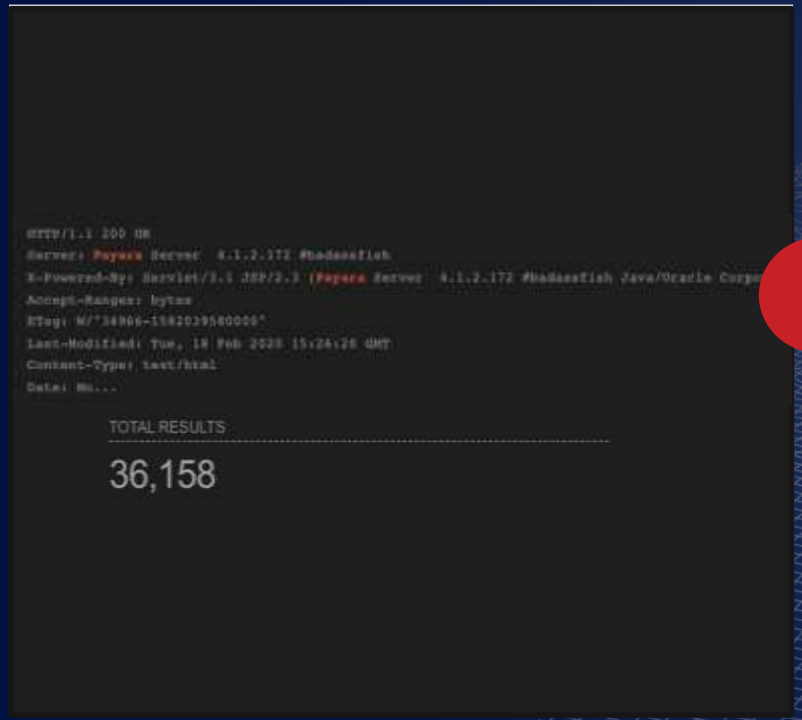


Attackers Perspective

Target Temptation

Applicability	Level of Adoption.	Exploitability	Susceptibility to Weakness.
Criticality	Security Boundary.	Research Potential	Ease of Development.
Enumerability	Enumerability.	Post Exploit Potential	Environment after Compromise.

Applicability: Level of Adoption

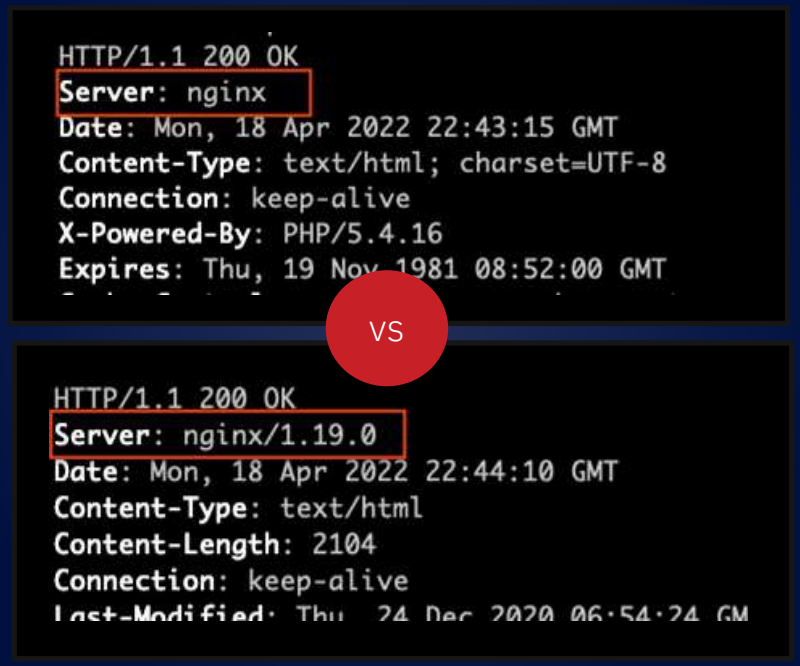


VS

Criticality: Security Boundary

VS

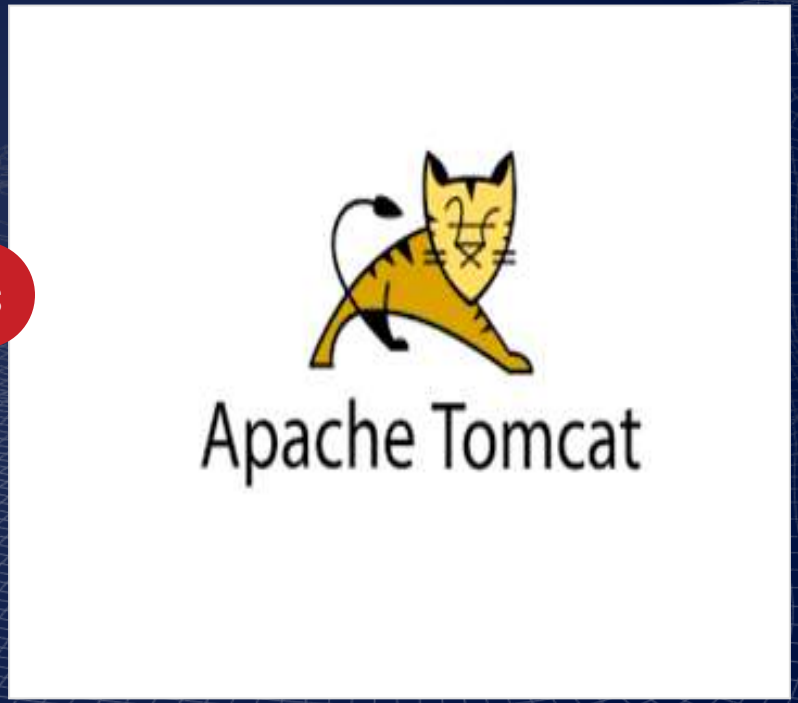
Enumerability: Precision of Detection



> The more information an attacker can glean from their external reconnaissance, the easier it is to target an asset

Exploitability: Susceptibility to Weakness

VS



Research Potential: Ease of Development

VS

Post Exploit Potential: Environment After Compromise

VS

Characteristic Rules: Temptation Modifier

Every algorithm requires adjustability:

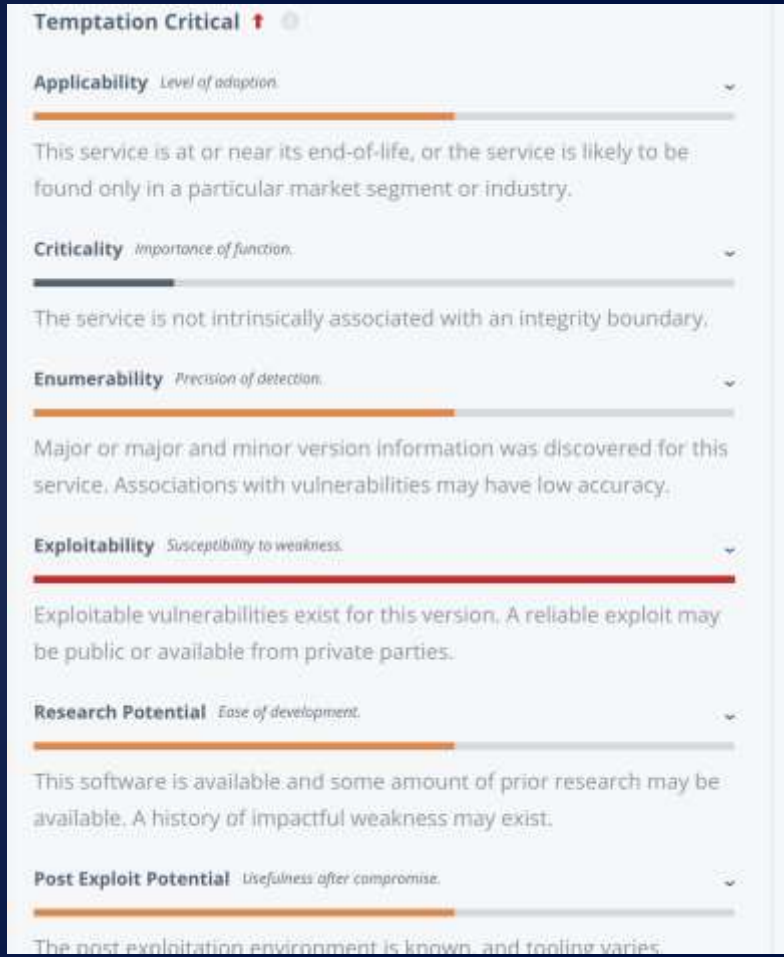
- ✓ Directory Listing
- ✓ Default Installation Page
- ✓ Login Page
- ✓ Old Copyright
- ✓ SSO Portal

Randori

The Attackers Perspective

Temptation drives stronger risk-based decisions relative to CVSS due to:

- ✓ Adversarial Context
- ✓ Multi Faceted Scoring
- ✓ User Adjustable Score



Practical Application: OpenSSL

Defenders See Vulnerabilities

CRITICAL CVSS

VS

Attackers See Targets

MEDIUM TEMPTATION

Randori, A Unified Offensive Security Platform

A Unified Offensive Security Platform

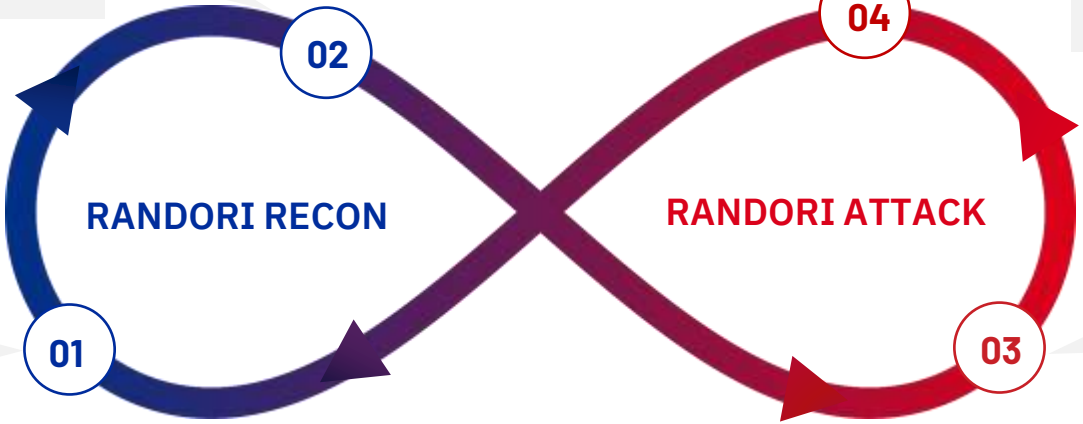
Build Resilience with Unified Offensive Security

PRIORITIZE

"Understand what an Adversary would Target"

VALIDATE

"Test your Defenses like an Adversary"



DISCOVER

"See your Attack Surface like an Adversary"

AUTHORIZE

"Scope your most relevant assets for attack emulation"

The Randori Factor: Differentiation

Randori empowers defenders to **operate with confidence**.

High Fidelity Discovery	Actionable Context	Low Friction Operations
Black-box reconnaissance designed to accurately identify your exposures including IPv6 assets.	Correlated findings with adversarial context designed to reduce alert fatigue and get you on target faster.	Drive action through bi-directional integrations that connect with your existing security stack.

Thank You.

Get a personal Attack Surface Review today
https://www.randori.com/demo/attack-surface/

an IBM Company