



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.

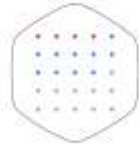
“

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

Point of View

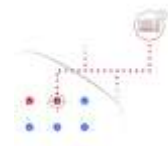
Defenders See Vulnerabilities



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

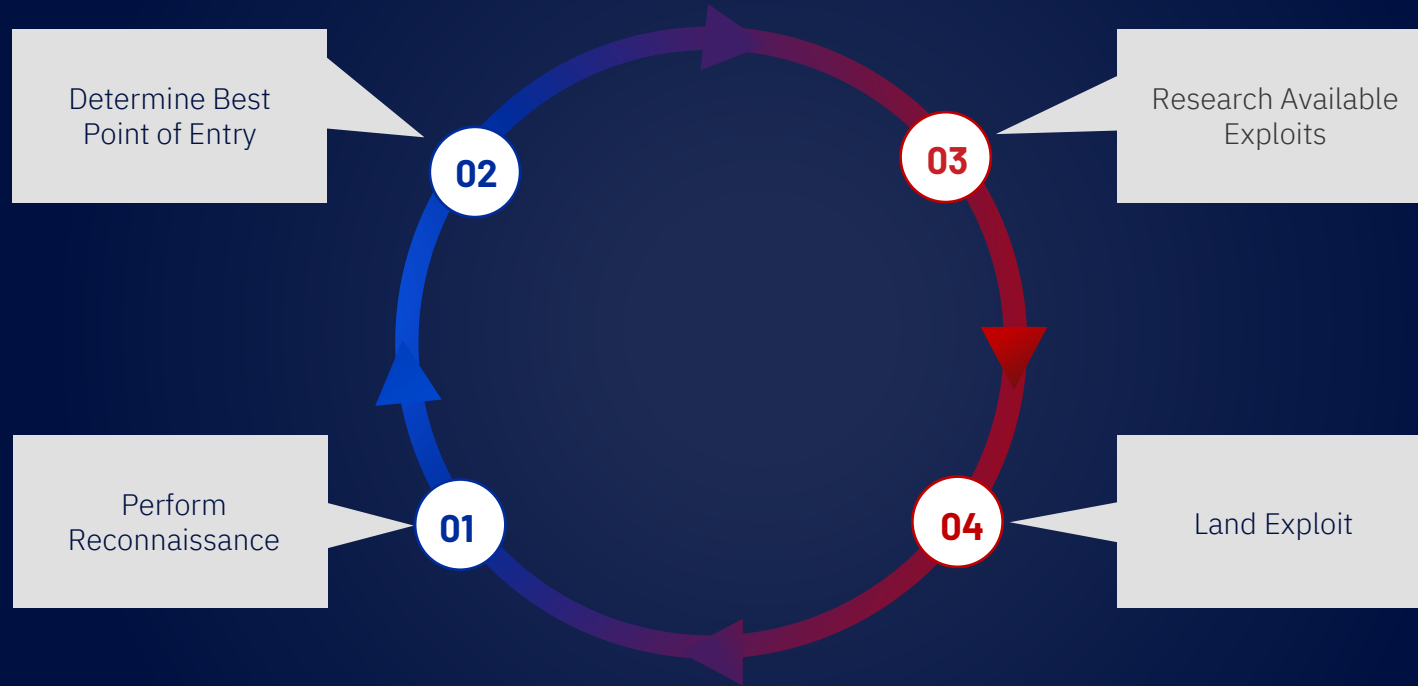
VS

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

```
HTTP/1.1 200 OK
Server: Payara Server 4.1.2.172 #badaassfish
X-Powered-By: Servlet/3.1 JSP/3.1 (Payara Server 4.1.2.172 #badaassfish Java/Oracle Corporation)
Accept-Ranges: bytes
ETag: W/"34966-158101980056"
Last-Modified: Tue, 18 Feb 2020 15:24:28 GMT
Content-Type: text/html
Date: Mon, 18 Apr 2022 18:05:09 GMT
```

TOTAL RESULTS

36,158

VS

```
HTTP/1.1 200
X-Powered-By: Servlet/5.0 JSP/3.0 (Apache Tomcat/10.0.4 Java/Oracle Corporation/14+36-)
Set-Cookie: JSESSIONID=7B1537976120E4A3CFA1342F656DFD73; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Content-Length: 1268
Date: Mon, 18 Apr 2022 18:05:09 GMT
Server: ...
```

TOTAL RESULTS

1,719,558

Criticality: Security Boundary



VS



Enumerability: Precision of Detection

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 18 Apr 2022 22:43:15 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

VS

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 18 Apr 2022 22:44:10 GMT
Content-Type: text/html
Content-Length: 2104
Connection: keep-alive
Last-Modified: Thu, 24 Dec 2020 06:54:24 GM
```

“

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

”

Exploitability: Susceptibility to Weakness



VS



Apache Tomcat

Research Potential: Ease of Development



GlobalProtect™

VS



Apache Tomcat

Post Exploit Potential: Environment After Compromise



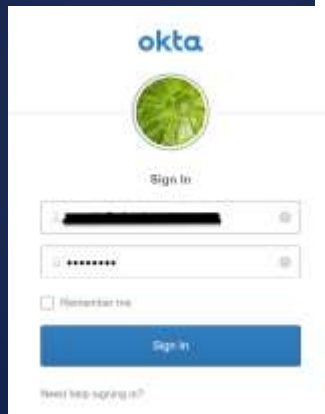
VS








Characteristic Rules: Temptation Modifier

Every algorithm requires adjustability:

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



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 secret/	2017-01-27 15:40	-	
 priv/	2017-01-27 15:41	-	
 edit/	2017-01-27 15:40	-	
 dir/	2017-01-27 15:40	-	
 config.php	2017-01-27 15:40	11K	

Apache/2.4.23 (Win64) PHP/5.6.25 Server at localhost Port 80

The Attackers Perspective

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

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

Temptation Critical ↑

Applicability *Level of adaption.*

This service is at or near its end-of-life, or the service is likely to be found only in a particular market segment or industry.

Criticality *Importance of function.*

The service is not intrinsically associated with an integrity boundary.

Enumerability *Precision of detection.*

Major or major and minor version information was discovered for this service. Associations with vulnerabilities may have low accuracy.

Exploitability *Susceptibility to weakness.*

Exploitable vulnerabilities exist for this version. A reliable exploit may be public or available from private parties.

Research Potential *Ease of development.*

This software is available and some amount of prior research may be available. A history of impactful weakness may exist.

Post Exploit Potential *Usefulness after compromise.*

The post exploitation environment is known, and tooling varies.

Practical Application: OpenSSL

Defenders See Vulnerabilities

CRITICAL CVSS

CVE-2022-3602 Detail

Current Description

A buffer overflow can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (leaving a client of service) or potentially remote code execution. Many platforms implement stack overflow protections which could mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. The announcements of CVE-2022-3602 described the issue as CVE-2022-3602. Further analysis based on some of the mitigating factors described above have led this to be downgraded to MSRN. Gains are not encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected: 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6).

Python Advisory Description

Severity: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:C/A:N

CVSS 3.1 Severity and Metrics

Base Score: Critical

Version: CVE-2022-3602 (Python/CVE-2022-3602)



Attackers See Targets

MEDIUM TEMPTATION

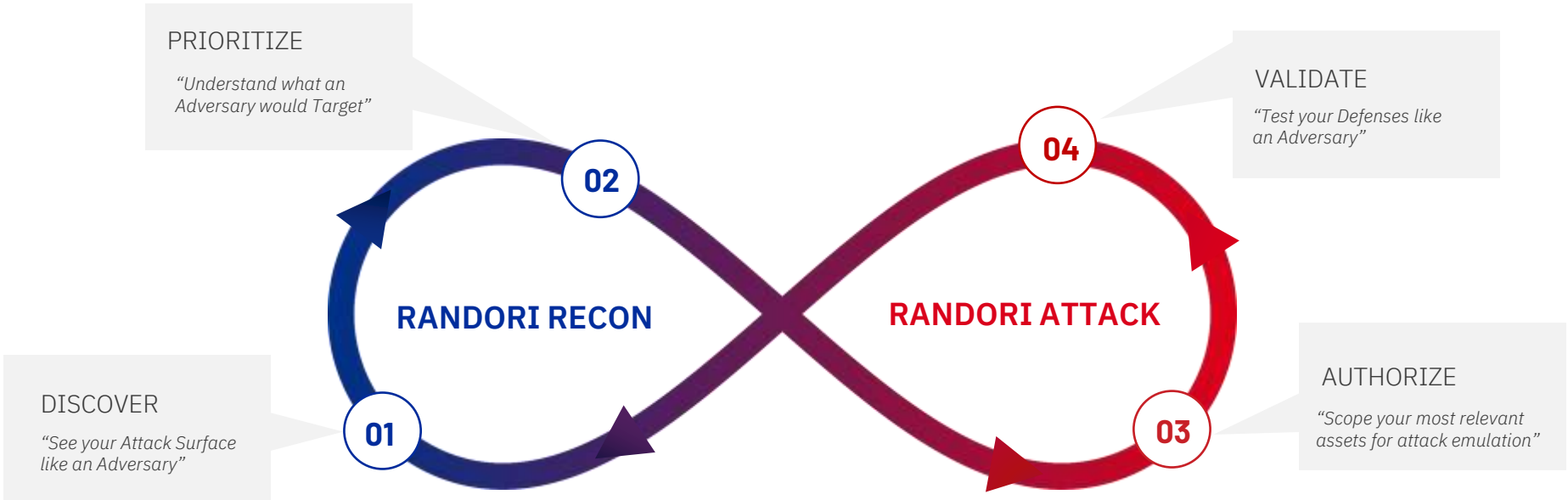


Randori, A Unified Offensive Security Platform

A Unified Offensive Security Platform



Build Resilience with Unified Offensive Security



The Randori Factor: Differentiation

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

High Fidelity Discovery

Black-box reconnaissance designed to accurately identify your exposures including IPv6 assets.

Actionable Context

Correlated findings with adversarial context designed to reduce alert fatigue and get you on target faster.

Low Friction Operations

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