BLACKWALL
SECURITY

KAORS
Penetration Test Report

Client	Sample Client (Demo Data)
Engagement Type	Grey-Box
Operator	Christian Chavez
Authorized By	J. Smith, CISO
Target	10.0.0.15
Assessment Date	2026-06-12
Engagement Start	N/A
Engagement End	N/A
Report ID	20260612_010240
Generated	2026-06-12 01:02 UTC

Scope — In Scope Targets

- 10.0.0.15

Penetration Test Report

Target: 10.0.0.15 | Date: 2026-06-12 | Classification: CONFIDENTIAL

Executive Summary

PREPARED FOR EXECUTIVE REVIEW — CONFIDENTIAL

Automated penetration test conducted against 10.0.0.15. 1 finding(s) identified: 1 critical, 1 high severity. Immediate remediation is required for all critical findings.

Risk Matrix

Each finding is plotted according to its assessed likelihood of exploitation and potential business impact. Findings confirmed through active exploitation are assigned maximum likelihood (5). Risk scoring follows CVSS 3.1 methodology.

LIKELIHOOD (rows) ↑

	Minimal (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)					
Likely (4)					1
Possible (3)					
Unlikely (2)					
Rare (1)					

IMPACT (columns) →

CRITICAL (15-25)	HIGH (8-14)	MEDIUM (4-7)	LOW (1-3)

Finding Index

#	Finding	Severity	CVSS	Position
1	vsftpd 2.3.4 backdoor	Critical	9.8	L4/I5

Field	Value
Target	10.0.0.15
Assessment Date	2026-06-12
Overall Risk Level	CRITICAL
Findings Identified	1
Critical Findings	1
Commands Executed	0

Scope

In-Scope Targets:

• 10.0.0.15

Discovered Services

No services recorded.

Risk Rating Methodology

Rating	CVSS 3.1 Score	Description
Critical	9.0 – 10.0	Immediate exploitation likely; critical business or data impact.
High	7.0 – 8.9	Significant risk; exploitation possible with moderate effort.
Medium	4.0 – 6.9	Moderate risk; exploitation requires specific conditions.
Low	0.1 – 3.9	Minimal risk; limited impact or highly unlikely exploitation.

All vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) version 3.1 base score. CVSS scores represent the intrinsic characteristics of a vulnerability and do not account for environmental or temporal factors specific to the target organization.

Where applicable, findings are mapped to the MITRE ATT&CK® framework to provide standardized adversary technique classification. MITRE ATT&CK technique IDs (e.g. T1190 – Exploit Public-Facing Application) allow defenders to cross-reference detections, threat intelligence, and mitigations within the ATT&CK knowledge base.

Identified Attack Paths

No attack paths identified.

Remediation Recommendations

Findings by MITRE Tactic

MITRE Tactic	Count	Description
Initial Access	1	Techniques to gain a foothold in the network

Finding	Severity	Recommendation	Priority	CVSS	CVE
vsftpd 2.3.4 backdoor	Critical	Upgrade vsftpd	P1 – Immediate	9.8	CVE-2011-2523

N/A in the CVE column = no CVE assigned. These findings represent configuration weaknesses, end-of-life software with no single applicable CVE, or misconfigurations referenced by CWE/OWASP rather than a named CVE identifier.

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Findings Affected
Initial Access	T1190	Exploit Public-Facing Application	vsftpd 2.3.4 backdoor

Chain of Custody

Field	Value
Operator	Christian Chavez
Client	Sample Client (Demo Data)
Authorized By	J. Smith, CISO
Engagement ID	N/A
Session ID	N/A
Target	10.0.0.15
Assessment Date	2026-06-12
Report ID	
Standard	NIST SP 800-115

All findings in this report were obtained through authorized testing as documented in engagement N/A. This chain of custody record is maintained in compliance with NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

Operator: Christian Chavez
Assessment Date: 2026-06-12
Signature: _____