



COMPANY PROFILE

Presented by: -

Date: 2025

Why Us?



Field Experienced

- ✔ Subject matter expertise
- ✔ Dedicated research-based penetration testers
- ✔ 8-12 years for assigned resource
- ✔ World recognized certifications
- ✔ Understanding challenges

Tailor Made Attacks

- ✔ Research based red teaming and penetration testing
- ✔ Customized attacks to find your organization
- ✔ World class benchmarking on threat posture
- ✔ Impact analyses of attacks
- ✔ Actionable remediation

Bespoke Learning

- ✔ Latest attack and optimized training for your demand
- ✔ Hands on exercises / Hacking
- ✔ Can be close to your organization
- ✔ Digitally enabled platform
- ✔ Learn how to detect

Offensive Security – Training



- ✓ Red Teaming
- ✓ Application Penetration Testing
- ✓ Infrastructure Penetration Testing

- ✓ Wireless Security Assessment
- ✓ Cloud Security Training
- ✓ SOC Analyst and DF / IR
- ✓ Threat Modelling

Penetration Testing Services



- ✓ Red Teaming
- ✓ Social Engineering
- ✓ Application Penetration Testing
- ✓ Infrastructure Penetration Testing
- ✓ Table-Top Exercise

- ✓ Wireless Security Assessment
- ✓ Digital Forensic Services
- ✓ OT Security Assessment

Red Teaming



- ✓ Objective Oriented
- ✓ Physical Security Assessment
- ✓ Against Specific TTP
- ✓ Custom as per Organization

Red Teaming Approach







Initiation of Project

-  Settings
-  Objectives
-  Approach
-  Planning




Identifying Targets

-  Network
-  Applications
-  People
-  Physical Access



Attack Simulation

-  Malware Development
-  Attack Design
-  Persistence



Reporting

-  Reporting
-  Evaluation of Risks

Security Training Platform

Hands On



- ▶ Access to the Lab
- ▶ VPN connection
- ▶ Choose your tools as you wish

See your Attacks



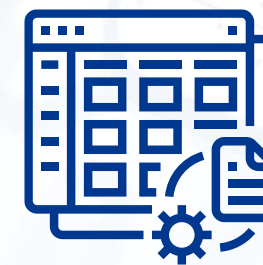
- ▶ View your attacks on the dashboard
- ▶ Analyse events
- ▶ Create detection signatures

Real Attacks



- ▶ You will perform attacks on servers and machines to simulate threat

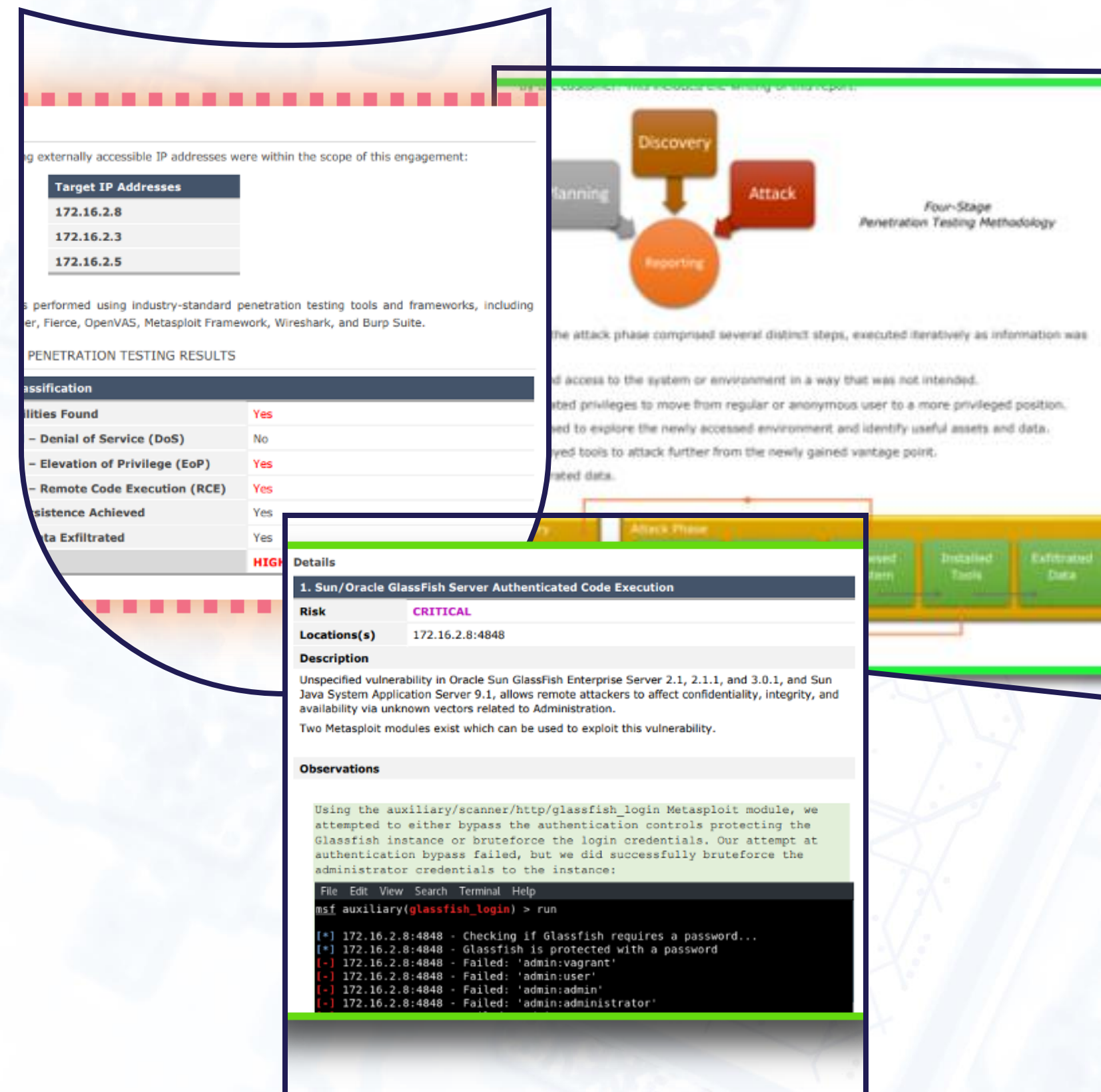
Task Management Platform



- ▶ Upload your evidence on the platform
- ▶ See hints and tutorials on the go

Deliverables

- Comprehensive Report
- Report Walkthrough
- Management Presentation
- Proof of Concept and evidence
- Remediation to mitigate attacks
- Top 4 – Attack Playbooks
- Top 4 – SPL on how to detect



g externally accessible IP addresses were within the scope of this engagement:

Target IP Addresses
172.16.2.8
172.16.2.3
172.16.2.5

is performed using industry-standard penetration testing tools and frameworks, including er, Fierce, OpenVAS, Metasploit Framework, Wireshark, and Burp Suite.

PENETRATION TESTING RESULTS

Classification	Findings
Privileges Found	Yes
- Denial of Service (DoS)	No
- Elevation of Privilege (EoP)	Yes
- Remote Code Execution (RCE)	Yes
Existence Achieved	Yes
Data Exfiltrated	Yes

Details

1. Sun/Oracle GlassFish Server Authenticated Code Execution

Risk CRITICAL

Locations(s) 172.16.2.8:4848

Description
 Unspecified vulnerability in Oracle Sun GlassFish Enterprise Server 2.1, 2.1.1, and 3.0.1, and Sun Java System Application Server 9.1, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Administration.
 Two Metasploit modules exist which can be used to exploit this vulnerability.

Observations

Using the auxiliary/scanner/http/glassfish_login Metasploit module, we attempted to either bypass the authentication controls protecting the Glassfish instance or bruteforce the login credentials. Our attempt at authentication bypass failed, but we did successfully bruteforce the administrator credentials to the instance:

```
File Edit View Search Terminal Help
msf auxiliary(glassfish_login) > run

[*] 172.16.2.8:4848 - Checking if Glassfish requires a password...
[*] 172.16.2.8:4848 - Glassfish is protected with a password
[-] 172.16.2.8:4848 - Failed: 'admin:vagrant'
[-] 172.16.2.8:4848 - Failed: 'admin:user'
[-] 172.16.2.8:4848 - Failed: 'admin:admin'
[-] 172.16.2.8:4848 - Failed: 'admin:administrator'
```


Zero Days



Free Software

- ✓ IE Browser
- ✓ Linux Kernel
- ✓ Android Kernel
- ✓ Wordpress CMS
- ✓ Joomla CMS
- ✓ Oracle DB
- ✓ and more



- ✓ Infernal wireless
- ✓ Free reconnaissance services

Our References



SimpleRisk



open source



TESLA

Google



Crypt Exchange
Platform



Government
Training and
Education



Our References

- Qnap
- Averda
- Bluesec
- NetSoft Solutions
- National CERT of Uzbekistan
- Alpha Group
- Aurora Aviation SA



Public Contribution

- Bit Breach – SG Community Education
- International Speaking at:
 - Black Hat
 - Japan SECCON
 - Null Dubai
 - HITB
 - TyphoonCon
- Continuous Zero Day Contribution to Vendors

