Advanced Pentest Service

Security Test Services

NETAŞ

2023

Penetration Testing is a security audit performed as unauthorized access to systems by detecting and exploiting vulnerabilities arising from human, logical and coding errors on systems.

The aim is to ensure that vulnerabilities are detected and eliminated before they are exploited by malicious people. Difference of the Pentest service from the classical Vulnerability scanning service is to exploit the vulnerabilities and to obtain and prove unauthorized access to the systems.

www.netas.com.tr

Pentest Services

- Web and Mobile Application Penetration Test
- Internal and External Network Penetration Test
- Wireless Network Penetration Test
- IoT / ATM Penetration Test
- Cloud Penetration Test
- API/Endpoint Client Penetration Test
- Red Team & Social Engineering Test
- DDoS Attack Simulation Test

NETAS

Why Do You Need Penetration Testing Service?

- The motivation of the attackers (Hacker) is above the motivation of the security experts. For this reason, security assessments without an attack-based security perspective remain incomplete.
- Prestige and financial losses experienced by institutions with increasing cyber attacks and critical data leaks in the world.
- Service interruptions in critical systems with DDoS attacks
- Competence/awareness deficiencies of the institution personnel
- In accordance with the legislation, institutions are obliged to have a Penetration Test, etc. ISO 27001, PCI DSS, BRSA, EMRA, HIPAA
- In the Web and Mobile Application development stages, Penetration Tests have become "one of the indispensable project steps" in the last stages of Network infrastructure and Server Systems before they are taken to live environments.

NETAS

Penetration Test Outputs

- Detection of malicious activities that the authorized users of the institution can do knowingly or unknowingly
- Measuring the security level of the institution against attacks by other malicious users (hackers) over the internal and external network
- Intelligence information sharing with the detection of sensitive information about the institution over the Internet
- Detection of whether more critical information has been accessed through the compromised systems
- Measuring the awareness of corporate employees against Social Engineering Attacks
- Measuring the security compliance status of the organization according to the Regulations
- We present Penetration Test Reports in 2 different sections as Technical and Management reports.

NETAS

Our Pentest Team Certificates

Our experts have International certifications. In addition, They is constantly researching new vulnerabilities and attack techniques.

GPEN
(GIAC Penetration Tester)

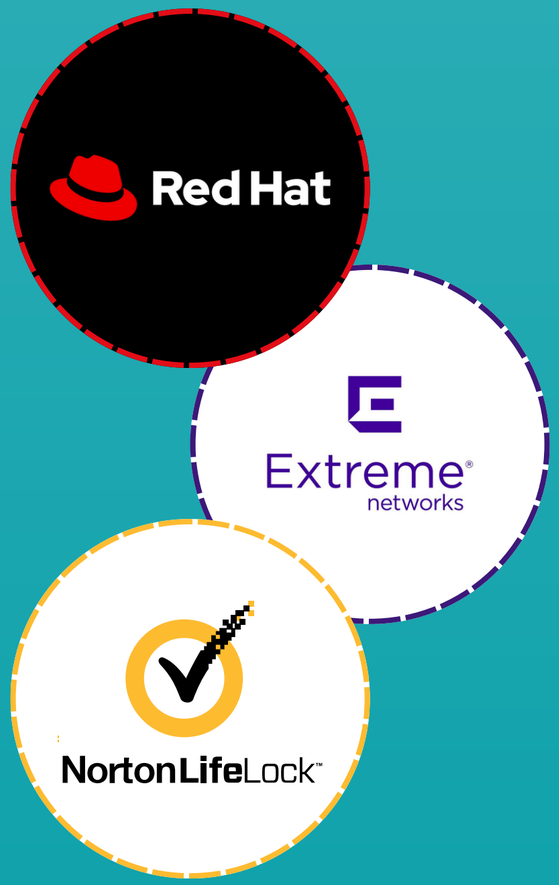
CEH
(Certified Ethical Hacker)

OSCP
(Offensive Security Certified Professional)

TSE B Layer Approved Penetration Testing

ITIL-F (Information Technologies Infrastructure Library)

www.netas.com.tr



Our Bug Bounty Vulnerabilities

- **CVE-2022-2256: RedHat Keycloak Open Source Identity and Access Management** - Stored XSS Vulnerability
- **CVE-2020-18305: Extreme Networks Switch EXOS Chalet Web GUI** - Privilege Escalation Vulnerability
- **CVE-2019-18373: Norton App Lock** - Security Passcode/Pattern Lock Screen Bypass Vulnerability

NETAS

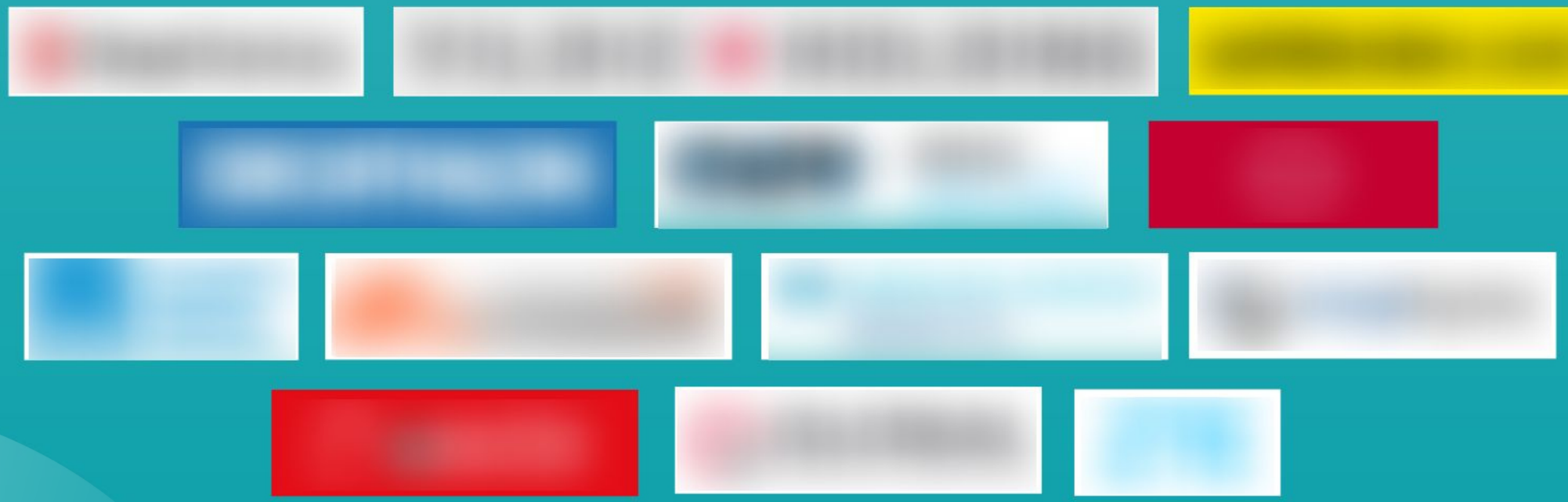
Our Hall of Fame Achievements

- **Philips - Hall of Fame** https://www.philips.com/a-w/security/coordinated-vulnerability-disclosure/hall-of-honors.html
- **BlackBerry - Hall of Fame** https://www.blackberry.com/us/en/services/blackberry-product-security-incident-response
- **Bosch - Hall of Fame** https://psirt.bosch.com/hall-of-fame/bosch-products-hall-of-fame/
- **Asus - Hall of Fame** https://www.asus.com/content/ASUS-Product-Security-Advisory/
- **Avrupa Birliği - Hall of Fame** https://cert.europa.eu/cert/newsletter/en/latest_HallOfFame_.html
- **Deutsche Telekom - Hall of Fame** https://www.telekom.com/en/corporate-responsibility/data-protection-data-security/security/details/acknowledgements-358300
- **Stanford University - Cross Site Scripting**
- **Harvard University - HTML Injection**

NETAS

Our references

We are trusted by the largest companies in the industry for pentest service.
Due to NDA agreements, reference information cannot be shared in writing.
You can get information from your Netaş Sales representative.



www.netas.com.tr

2021-2022 Pentest Projects

- **Finance Sector –** All domestic and foreign institutions IT Infrastructure, DDoS
- **Holdings –** All domestic and foreign institutions IT Infrastructure
- **E-Commerce –** IT Infrastructure
- **International Merchandising –** Web/Mobile Applications
- **Aviation Logistics Industry –** Entire IT Infrastructure, DDoS
- **Automotive –** Web/Mobile Applications
- **Aviation Industry –** Entire IT Infrastructure, DDoS
- **R&D –** Web Application
- **Institutions from Many Various Sectors –** Web/Mobile Application
- **Capital Markets –** Entire IT Infrastructure, DDoS
- **Telecom Industry –** Web Application, DDoS

NETAS

Pentest Methodology

Test Methodology and Standards

- OWASP Application Security Verification Standard (ASVS)
- OWASP Mobile Application Security Verification Standard (MASVS)
- OWASP Firmware Security Testing Methodology
- “OSSTMM” Open Source Security Testing Methodology Manual
- TS 13638, PCI Penetration testing, ISSAF, NIST SP800-115

Our Approach

- We follow **creative** penetration testing approaches with our own **manual research** to uncover vulnerabilities that automated tools miss.

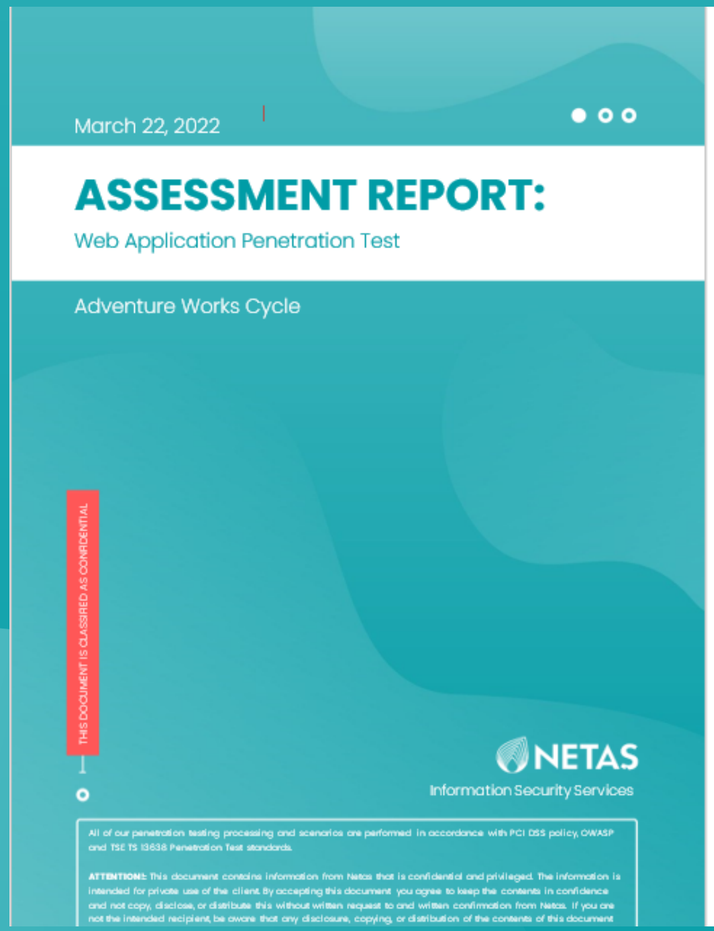
- By detecting all architectures, endpoints and parameters on applications, we aim to address the **attack surface** more comprehensively and to reveal **all possible attack scenarios.**

- We carry out the entire penetration test process in a **controlled** manner so that the daily functioning of **your institution is not affected.**

Report Outputs

www.netas.com.tr

We ensure that the vulnerability findings shared as a result of the penetration test are valid, **reproducible**, **high quality** and **actionable** outputs.



March 22, 2022

ASSESSMENT REPORT:

Web Application Penetration Test

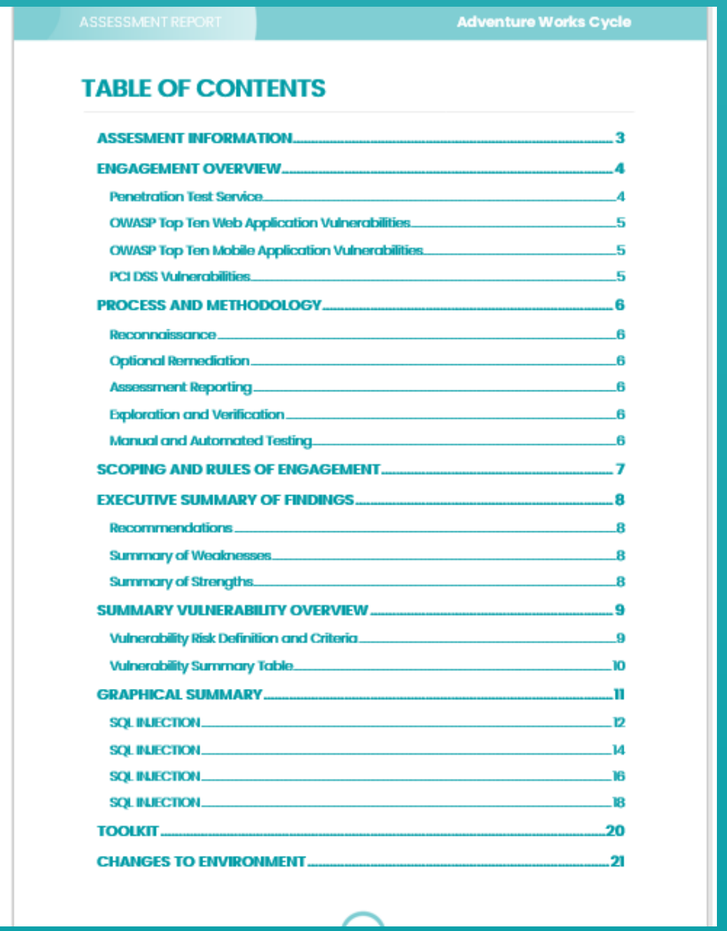
Adventure Works Cycle

THIS DOCUMENT IS CLASSIFIED AS CONFIDENTIAL

NETAS
Information Security Services

All of our penetration testing processing and scenarios are performed in accordance with PCI DSS policy, OWASP and TSE TS 13638 Penetration Test standards.

ATTENTION: This document contains information from Netas that is confidential and privileged. The information is intended for private use of the client. By accepting this document you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from Netas. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document



ASSESSMENT REPORT Adventure Works Cycle

TABLE OF CONTENTS

ASSESMENT INFORMATION 3
ENGAGEMENT OVERVIEW 4
Penetration Test Service 4
OWASP Top Ten Web Application Vulnerabilities 5
OWASP Top Ten Mobile Application Vulnerabilities 5
PCI DSS Vulnerabilities 5
PROCESS AND METHODOLOGY 6
Reconnaissance 6
Optional Remediation 6
Assessment Reporting 6
Exploration and Verification 6
Manual and Automated Testing 6
SCOPING AND RULES OF ENGAGEMENT 7
EXECUTIVE SUMMARY OF FINDINGS 8
Recommendations 8
Summary of Weaknesses 8
Summary of Strengths 8
SUMMARY VULNERABILITY OVERVIEW 9
Vulnerability Risk Definition and Criteria 9
Vulnerability Summary Table 10
GRAPHICAL SUMMARY 11
SQL INJECTION 12
SQL INJECTION 14
SQL INJECTION 16
SQL INJECTION 18
TOOLKIT 20
CHANGES TO ENVIRONMENT 21

ASSESSMENT REPORT Adventure Works Cycle

EXECUTIVE SUMMARY OF FINDINGS

NETAS conducted a Penetration Test for **Adventure Works Cycle**. This test was performed to assess **Contoso**'s defensive posture and provide security assistance through proactively identifying vulnerabilities, validating their severity, and providing remediation steps.

NETAS reviewed the security of **Adventure Works Cycle**'s infrastructure and has determined a Critical risk of compromise from external attackers, as shown by the presence of the vulnerabilities detailed in this report. The detailed findings and remediation recommendations for these assessments may be found later in the report.

OWASP Web Top 10 Penetration Test — 3 CRITICAL RISK FOUND!

PCI-DSS Penetration Test — 3 CRITICAL RISK FOUND!

OWASP Mobile Top 10 Penetration Test — 3 CRITICAL RISK FOUND!

Summary of Strengths

NETAS was tasked with finding issues and vulnerabilities dealing with the current environment. It is useful to know when positive findings appear. Understanding the strengths of the current environment can reinforce security best practices and provide strategy and direction toward a robust defensive posture. The following traits were identified as strengths in Contoso's environment.

1. Proper implementation of Two-Factor Authentication (2FA) for login forms.
2. Passwords in database are hashed using a strong algorithm.
3. Strong access controls in place for each user role.

Summary of Weaknesses

NETAS discovered and investigated many vulnerabilities during the course of its assessments for Adventure Works Cycle. We have categorized these vulnerabilities into general weaknesses across the current environment,and provide direction toward remediation for a more secure enterprise.

1. Poor sanitation of user input lead to multiple vulnerabilities.
2. Application running as root on server and has permissions to files it shouldn't need to access.
3. Lack of brute force protection on login forms.

Recommendations

Not all security weaknesses are technical in nature, nor can they all be remediated by security personnel. Companies often have to focus on the root security issues and resolve them at their core. These strategic steps are changes to the operational policy of the organization. **NETAS** recommends the following strategic steps for improving the company's security.

1. Ensure proper development and repository practices by in-house and 3rd party developers.
2. Require authentication for publicly accessible pages and directories that have sensitive information.
3. Remove legacy servers, subdomains, pages, and other web resources no longer in use.
4. Sanitize all user inputs before processing it on the server side of the application.
5. Enhance security defenses with additional detection and response capabilities, such as a SIEM.

Report Outputs

The vulnerabilities found are divided into 5 categories as "**Critical**", "**High**", "**Medium**", "**Low**" and "**Best Practices**" according to their importance level. A detailed description of each vulnerability, the description, affected platforms, remediation methods, and any references to the related vulnerability, set out in the report.

Vulnerability Summary Table

The findings determined as a result of the security audit are classified and presented visually in this section.

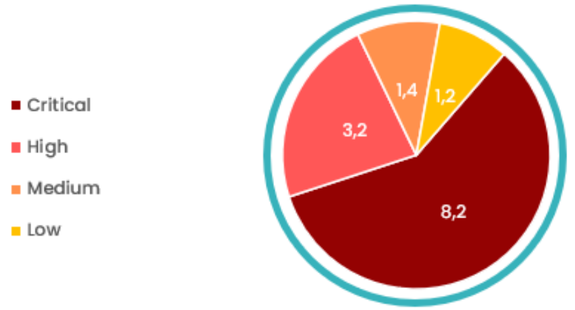
3	3	3	3	3
CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK	BEST PRACTICES

The following vulnerabilities were found within each risk level. It is important to know that total vulnerabilities is not a factor in determining risk level. Risk level is depends upon the severity of the vulnerabilities found.

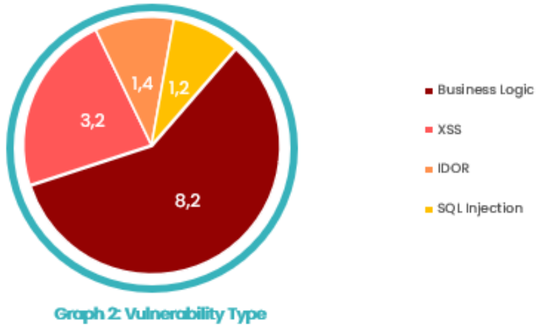
Vulnerability ID – Name And Remediation	Severity	Risk Level
CI – SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		CRITICAL
HI – SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		HIGH
MI – SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		MEDIUM
MI – SQL INJECTION Use parameterized queries (also known as prepared statements) for all database queries.		LOW

GRAPHICAL SUMMARY

The below graphical representations from **NETAS** will provide you an overall summary of the security audit scan results, including, vulnerabilities discovered, severity respective CVSS Score, and other vulnerability details such as its impact, detailed PoC, steps to reproduce, affected URLs/network parameters, and recommended fixes.



Graph 1: Severity Type



Graph 2: Vulnerability Type

NETAS

Report Outputs

H1	Stealing OAuth Tokens via an Insecure Open Redirect	HIGH ⚠
Vuln. Type(s)	Insecure Redirect	
Access Point(s)	External	
Attacker Profile	Anonymous	

C1	SQL INJECTION	CRITICAL
Vuln. Type(s)	Insufficient Input Validation	
Access Point(s)	External	
Attacker Profile	Anonymous	
Affected Host(s)	http://admin.contoso.com/search.php?id=1	
Impact(s)	Remote Code Execution, Information Disclosure	
Description	SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query. This kind of attack can be detrimental to client and company data. A wide range of damaging attacks can often be delivered via SQL injection, including reading, adding, modifying, or deleting critical application data, interfering with application logic, escalating privileges within the database and executing commands on the underlying operating system.	
Detail(s)	This vulnerability was detected by fuzzing the vulnerable parameters with a variety of malicious input until an unexpected response was returned. The assessor navigated to /search.php and noted a verbose SQL error message and saw where the "id" parameter was being injected into the SQL Query. Using sqlmap the assessor extracted the user's table from the public database with the payload **';select * from users**	
Proof(s)		
Remediation(s)	You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective: • One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because	

NETAS

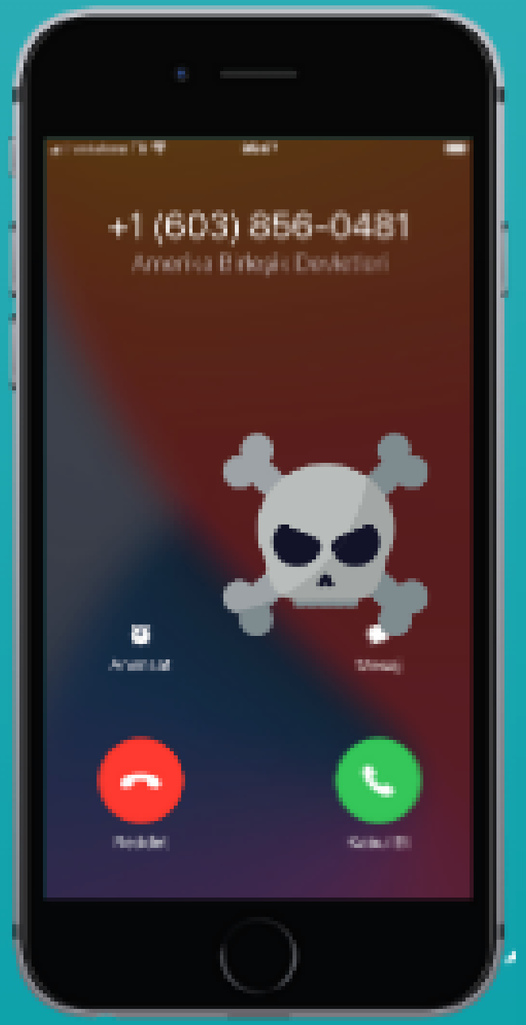
www.netas.com.tr

DoS/DDoS Distributed Denial of Service Attack Simulations

- **Volumetric:** UDP-ICMP bandwidth, Tcp Syn, Ack, Psh+Ack, Rst Flood, DNS, NTP, SNMP, Portmap, Netbios, RIPv1 Amplification
- **DNS Attacks:** DNS Flood, DNS Amplification
- **Layer 7:** Http, Https GET/POST Flood
- **System Resource Exploitation :** Ping of Death, Slow read, Sock stress, Tcp Syn-Fin, Rst Flood
- **BotNet:** Bot net attack simulation test with ICMP, UDP, TCP, http Flood attack techniques using hundreds of different IP sources.
- **Custom**: Special attack tests by creating scenarios and special attack types that we will mutually determine in accordance with your application, server and security systems.

NETAS

www.netas.com.tr



Advanced Attack Simulations

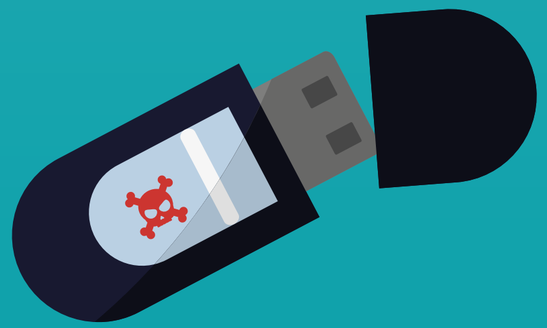
- Targeted Email Phishing Attacks
- Vishing (Voice Phishing) Attacks
- Red Teaming

NETAS

www.netas.com.tr

Test Tools

- Burp Suite Professional
- Nessus Professional, Nuclei
- Metasploit
- sqlmap, gobuster, amass, nmap
- aircrack-ng, wifijammer, bettercap, mitm-proxy, tcpdump, responder, mimikatz, crackmapexec
- binwalk, QEMU, EMBA, TROMMEL
- Our Custom script, Exploit and Hardware Tools



NETAS

NETAS

Thank You

İLKER BULGURCU

Team Lead, Security Testing Services

bulgurcu@netas.com.tr