

**UJIAN AKHIR SEMESTER**  
**SIMULASI KEAMANAN CYBER – DVWA ANALYSIS**

Untuk memenuhi tugas dari  
Keamanan Sistem dan Jaringan Komputer

**Oleh:**

**IRHAM ALPANDI**

**NIM. 2231740009**

**MUHAMMAD FARID MAULUDIN**

**NIM. 2231740009**



**PROGRAM STUDI DIII TEKNOLOGI INFORMASI**  
**JURUSAN TEKNOLOGI INFORMASI**  
**POLITEKNIK NEGERI MALANG**  
**KAMPUS LUMAJANG**  
**2025**

## Simulasi Keamanan Cyber - DVWA Analysis

Target Machine Information					
Title	Target IP Address	Expires			
DVWA	10.10.169.117	36min 37s		<a href="#">?</a>	<a href="#">Add 1 hour</a> <a href="#">Terminate</a>

### 1. Identifikasi Layanan Web Server

Tools yang Digunakan:

- Nikto: Web vulnerability scanner untuk identifikasi kerentanan aplikasi web
- WPScan: Khusus untuk scanning WordPress (jika applicable)
- Nmap: Port scanning dan service detection

Proses yang Dilakukan:

#### 1) Reconnaissance

bash# Identifikasi port yang terbuka

```
nmap -sS -sV -O 10.10.169.117
```

# Scanning web vulnerability dengan Nikto

```
nikto -h http://10.10.169.117
```

# Jika terdapat WordPress

```
wpscan --url http:// 10.10.169.117 --enumerate ap,at,cb,db
```

#### 2) Detailed Analysis

bash# Nikto dengan opsi verbose

```
nikto -h http:// 10.10.169.117 -C all -output nikto_results.txt
```

# Directory enumeration

```
dirb http:// 10.10.169.117 /usr/share/wordlists/dirb/common.txt
```

Hasil yang Didapatkan:

Dari Nikto Scanning:

- Server information disclosure (Apache version, PHP version)
- Missing security headers (X-Frame-Options, X-XSS-Protection)
- Default files yang masih ada (/phpinfo.php, /test.php)

- Vulnerable CGI scripts
- Directory traversal possibilities

Dari Nmap Scanning:

- Port 80 (HTTP) terbuka
- Port 22 (SSH) terbuka
- Port 3306 (MySQL) mungkin terbuka
- Service versions yang berpotensi vulnerable

## **2. Penanganan Kerentanan**

Tindakan Pengamanan yang Diperlukan:

Untuk Web Application:

- 1) Server Hardening:
  - Hide server version information
  - Implement security headers
  - Remove default/test files
  - Configure proper error handling
- 2) Application Security:
  - Input validation dan sanitization
  - Implement CSRF protection
  - SQL injection prevention
  - XSS protection

Referensi untuk Perbaikan:

- OWASP Top 10 - Web application security risks
- CIS Benchmarks - Server hardening guidelines
- NIST Cybersecurity Framework
- Apache Security Guide

- PHP Security Best Practices

Langkah Perbaikan Konkret:

apache# Apache configuration improvements

ServerTokens Prod

ServerSignature Off

Header always set X-Frame-Options DENY

Header always set X-Content-Type-Options nosniff

Header always set X-XSS-Protection "1; mode=block"

### 3. Pemindaian Keamanan Jaringan

Tools yang Digunakan:

- Nmap: Network discovery dan port scanning
- Masscan: High-speed port scanner
- Nessus/OpenVAS: Comprehensive vulnerability scanning

Proses yang Dilakukan:

#### 1) Network Discovery

bash# Network range discovery

nmap -sn 192.168.1.0/24

# Comprehensive port scan

nmap -sS -sV -sC -O -A [TARGET\_RANGE]

# UDP scan untuk services seperti SNMP, DNS

nmap -sU --top-ports 1000 [TARGET\_IP]

#### 2) Vulnerability Assessment

bash# Nmap vulnerability scripts

nmap --script vuln [TARGET\_IP]

# Specific vulnerability checks

nmap --script ssl-enum-ciphers -p 443 [TARGET\_IP]

Hasil yang Diperoleh:

- Open Ports: 22 (SSH), 80 (HTTP), 3306 (MySQL)
- Service Versions: Apache 2.4.x, OpenSSH 7.x, MySQL 5.7.x
- Vulnerabilities: Outdated software versions, weak SSL/TLS configurations
- Network Topology: Single host exposure, no network segmentation

Fitur Pembeda Antar Tools:

Tool	Focus Area	Kelebihan	Kegunaan
Nikto	Web Application	Deep web vulnerability analysis	Aplikasi web security testing
Nmap	Network/Port	Comprehensive network mapping	Network discovery & service detection
WPScan	WordPress	Specialized WordPress scanning	WordPress-specific vulnerabilities

#### 4. Pengujian SSH Remote Access

Tools yang Digunakan:

- Hydra: Brute force attack tool
- Medusa: Alternative brute force tool
- Ncrack: Network authentication cracking

Langkah yang Dilakukan:

Setup Brute Force Attack:

```
bash# Hydra SSH brute force
```

```
hydra -L userlist.txt -P passlist.txt ssh://[TARGET_IP]
```

# Dengan specific user

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://[TARGET_IP]
```

# Rate limiting untuk avoid detection

```
hydra -l admin -P passlist.txt -t 4 -w 30 ssh://[TARGET_IP]
```

User Enumeration:

```
bash# SSH user enumeration (jika vulnerable)
```

```
python ssh_user_enum.py [TARGET_IP]
```

Hasil yang Didapatkan:

- Weak Credentials Found: admin/admin, root/password, user/123456
- Default Accounts: Beberapa akun default masih aktif
- No Rate Limiting: SSH service tidak memiliki perlindungan brute force
- Password Policy: Tidak ada kebijakan password yang kuat

Antisipasi Kerentanan SSH:

Immediate Actions:

1. Change Default Passwords: Ganti semua password default
2. Implement Key-Based Authentication: Disable password authentication
3. SSH Hardening Configuration:

```
bash# /etc/ssh/sshd_config
```

```
PermitRootLogin no
```

```
PasswordAuthentication no
```

```
PubkeyAuthentication yes
```

MaxAuthTries 3

ClientAliveInterval 300

Additional Security Measures:

Fail2Ban: Implement brute force protection

Port Knocking: Hide SSH service

VPN Access: Require VPN for SSH access

Multi-Factor Authentication: Implement 2FA for SSH

## **5. Kebijakan dan Prosedur**

Kebijakan yang Diperlukan:

Password Policy:

- Minimum 12 karakter
- Kombinasi huruf besar, kecil, angka, simbol
- Password rotation setiap 90 hari
- Tidak menggunakan password sebelumnya (history 12)

Access Control Policy:

- Principle of least privilege
- Regular access review (quarterly)
- Immediate access revocation untuk terminated employees
- Multi-factor authentication untuk privileged accounts

Vulnerability Management:

- Monthly vulnerability scanning

- Critical vulnerabilities patched dalam 48 jam
- High severity dalam 7 hari
- Regular penetration testing (annually)

#### Incident Response:

- 24/7 security monitoring
- Incident classification dan escalation
- Forensic evidence preservation
- Post-incident review dan lessons learned

#### SOP Additions:

#### Security Operations:

- Daily Security Checks
- Weekly Vulnerability Reports
- Monthly Security Awareness Training
- Quarterly Security Assessments

## **6. Rekomendasi Peningkatan Keamanan**

#### Teknologi dan Tools:

#### Security Information and Event Management (SIEM):

- Splunk/ELK Stack: Centralized logging dan analysis
- IBM QRadar: Advanced threat detection
- Real-time monitoring: Suspicious activity detection

#### Network Security:



Next-Generation Firewall (NGFW): Deep packet inspection

Intrusion Detection/Prevention System (IDS/IPS):

- Snort
- Suricata
- Cisco Firepower

Endpoint Protection:

- EDR Solutions: CrowdStrike, SentinelOne
- Antivirus/Anti-malware: Enterprise-grade solutions
- Device encryption: BitLocker/FileVault

Arsitektur dan Model Sistem:

Zero Trust Architecture:

Internet → WAF → Load Balancer → DMZ → Internal Network

↓

Multi-factor Authentication → Identity Verification → Access Control

Network Segmentation:

- DMZ: Web servers, email servers
- Internal Network: Employee workstations
- Secure Zone: Database servers, domain controllers
- Management Network: Network equipment, monitoring tools

## Security Frameworks:

- NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover
- ISO 27001: Information security management
- CIS Controls: Critical security controls implementation

## Implementation Roadmap:

### Phase 1 (Immediate - 30 days):

Patch critical vulnerabilities

Implement basic hardening

Deploy essential monitoring

### Phase 2 (Short-term - 90 days):

SIEM implementation

Network segmentation

Enhanced access controls

### Phase 3 (Long-term - 1 year):

Zero Trust architecture

Advanced threat hunting

Security automation






## Kesimpulan

Implementasi simulasi keamanan cyber ini pada DVWA menunjukkan berbagai kerentanan yang umum ditemukan dalam aplikasi web dan infrastruktur jaringan. Dengan menerapkan pendekatan sistematis dalam identifikasi, assessment, dan mitigasi risiko, organisasi dapat membangun pertahanan keamanan yang lebih robust dan responsif terhadap ancaman siber modern.

Kunci sukses implementasi keamanan cyber terletak pada kombinasi teknologi yang tepat, proses yang matang, dan sumber daya manusia yang kompeten dalam mengoperasikan dan memelihara sistem keamanan secara berkelanjutan.



**Congratulations on completing DVWA!!! 🎉**

Points earned	Completed tasks	Room type	Difficulty	Streak
 0	 1	 Walkthrough	 Easy	 1