PENGUJIAN KEAMANAN SISTEM WEBSITE DENGAN TEKNIK PENETRATION TESTING DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

(STUDI KASUS : SUB DOMAIN UPNJATIM.AC.ID)

SKRIPSI

Oleh :

NICO NATANAEL

19081010023

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2023

LEMBAR PENGESAHAN
SKRIPSI

Judul : **PENGUJIAN KEAMANAN SISTEM WEBSITE DENGAN TEKNIK PENETRATION TESTING DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP)**

Oleh : **NICO NATANAEL**

NPM : **19081010023**

Telah Diseminarkan Dalam Ujian Skripsi Pada :

Hari Jum'at, Tanggal 10 November 2023

Mengetahui

Dosen Pembimbing

1.

Dr. Ir. Mohammad Idhom, SP, S.Kom, MT.

NIP : 19830310 2021211 006

2.

Achmad Junaidi, S.Kom, M.Kom

NPT : 3 7811 04 0199 1

Dosen Penguji

1.

Henni Endah Wahanani, ST, M.Kom

NIP : 19780922 2021212 005

2.

Firza Prima Aditiawan, S.Kom, M.TI

NIP : 19860523 2021211 003

Menyetujui

Dekan

Fakultas Ilmu Komputer

Prof. Dr. Ir. Novirina Hendrasarie, MT.

NIP : 19681126 199403 2 001

Koordinator Program Studi

Teknik Informatika

Fetty Tri Anggraeny, S.Kom, M.Kom

NIP : 19820211 2021212 005

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Program Studi Informatika UPN "Veteran" Jawa Timur, yang bertanda tangan di bawah ini :

Nama : Nico Natanael

NPM : 19081010023

Menyatakan bahwa judul skripsi yang saya ajukan dan kerjakan, dengan judul :

"PENGUJIAN KEAMANAN SISTEM WEBSITE DENGAN TEKNIK PENETRATION TESTING DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (STUDI KASUS : SUB DOMAIN UPNJATIM.AC.ID)"

Bukan merupakan plagiat dan skripsi/tugas akhir/penelitian orang lain dan juga bukan merupakan produk atau software yang saya beli dari pihak lain. Saya juga menyatakan bahwa skripsi ini adalah pekerjaan saya sendiri, kecuali yang dinyatakan dalam daftar pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN "Veteran" Jawa Timur maupun di institusi pendidikan lain. Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 20 November 2023

Penulis,

Nico Natanael

NPM : 19081010023

PENGUJIAN KEAMANAN SISTEM WEBSITE DENGAN TEKNIK PENETRATION TESTING DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Nama Mahasiswa : Nico Natanael
NPM : 19081010023
Program Studi : Informatika
Dosen Pembimbing : Mohammad Idhom, SP.,S.Kom., MT.
Achmad Junaidi, S.Kom, M.Kom

Abstrak

Penggunaan Website yang kian marak diberbagai bidang, seringkali melupakan hal evaluasi terkait keamanan website. Untuk mengevaluasi keamanan website terdapat Teknik yang bernama Penetration Testing. Teknik ini masih sangat memungkinkan untuk dipakai dalam hal mengevaluasi keamanan website. Terdapat penelitian terdahul yang menerangkan bahwa betapa jahatnya kejahatan cyber. Yang mana, dalam pengujian kelemahan website menggunakan teknik yang sama yaitu Web Penetration Testing. Diterangkan beberapa tahapan untuk menjalankan Penetration Testing dalam menguji keamanan website. Dan diuraikan beberapa alat yang dipakai untuk melakukan Penetration Testing.

Penelitian ini menjelaskan bagaimana cara mengetahui kerentanan kerentanan yang ada pada suatu website dengan menggunakan metode pengujian penetrasi untuk mengungkap kelemahan Website. Dengan berbagai tahapan yang akan dilalui seperti Pre-Engagement Interactions, Intelegence Gathering, Vulnerability Testing, Exploitation, Repoting, dan Rekomendasi.

Mendapatkan sebuah hasil celah keamanan yang dapat di eksploitasi secara umum. Dapat dikatakan bahwa setelah melalui tahapan tahapan penetrasi testing dengan target studi kasus yang ada, Teknik penetration testing masih layak dan memungkinkan untuk dipakai. Di dalamnya terdapat hasil celah celah keamanan yang disajikan, dan hasil eksploitasi yang telah dijalankan. Tidak lupa juga memberikan sebuah rekomendasi dan laporan terhadap hasil pengujian.

Kata Kunci : *Web Penetration Testing, OWASP, Keamanan Website*

KATA PENGANTAR

Terimakasih kepada Tuhan Yesus Kristus, yang telah memberikan kekuatan, kesabaran, dan hal hal yang tidak diduga selama pengerjaan skripsi ini. Atas kasih karunia-Nya penulis dapat menyelesaikan skripsi dengan judul :

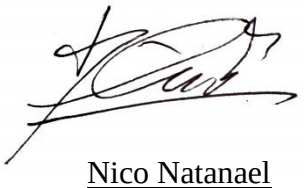
"Pengujian Keamanan Sistem Website Dengan Teknik Penetration Testing Dengan Metode Open Web Application Security Project (OWASP)"
(Studi Kasus : Sub Domain upnjatim.ac.id)

Selalu bersyukur atas orang orang baik disekitar penulis, dengan hal itu dapat memudahkan pengerjaan dan penulisan laporan skripsi ini. Banyak berharap dengan adanya laporan skripsi ini dapat menambah wawasan baru bagi pembaca.

Penulis menyadari masih terdapat banyak kekurangan pada laporan penelitian skripsi ini, oleh karena itu, penulis menerima segala bentuk kritik, saran, dan masukkan dari semua pihak yang bertujuan membangun penelitian ini menjadi lebih baik dan sempurna.

Surabaya, 20 November 2023

Penulis,



Nico Natanael

NPM. 19081010023

UCAPAN TERIMAKASIH

Atas kasih karunia Tuhan Yesus Kristus penelitian dan laporan ini berhasil terselesaikan. Selain itu dengan segala hormat, ucapan terimakasih yang sebesar-besarnya diucapkan kepada seluruh pihak terkait yang telah membantu atas selesainya laporan skripsi ini. Secara khusus penulis ingin menyampaikan ucapan terimakasih yang sebesar-besarnya kepada semua pihak yang telah membantu.

Pada Kesempatan ini penulis menyampaikan rasa terimakasih yang sebesar besarnya kepada :

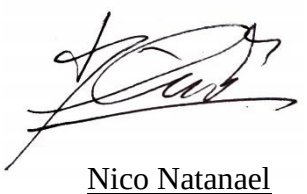
1. Tuhan Yesus Kristus yang telah memberikan kelancaran dan kemudahan kepada saya sehingga skripsi ini dimudahkan dan dilancarkan sampai selesai.
2. Papa dan Mama yang selalu memberikan dukungan baik materi dan non-materi, sehingga saya dapat menyelesaikan segala rintangan selama kuliah berlangsung.
3. Kakak satu satunya yang selalu memberikan bantuan baik secara materi dan non-materi sehingga saya dapat semangat menjalani perkuliahan dari awal hingga akhir.
4. Bapak Prof. Dr. Ir. Akhmad Fauzi, MMT selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Ibu Prof. Dr. Novirina Hendrasarie, S.T, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
6. Ibu Fetty Tri Anggraeny, S.Kom, M.Kom. selaku Koordinator Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur
7. Bapak Fawwaz Ali Akbar, S.Kom, M.Kom, selaku selaku dosen wali saya yang membantu perkuliahan dari awal hingga akhirnya.
8. Bapak Mohammad Idhom, SP., S.Kom., MT., selaku dosen pembimbing pertama saya, yang selalu memberikan bantuan, arahan, dan pandangan terkait skripsi saya. Tanpa beliau skripsi saya terasa hambar.
9. Bapak Achmad Junaidi, S.Kom, M.Kom., selaku dosen pembimbing dua saya, yang selalu memberikan tuntunan, pandangan, dan bantuan terkait skripsi saya. Tanpa beliau skripsi saya tidak akan terasa manis.

10. Seluruh Dosen Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur yang telah memberikan ilmu yang bermanfaat selama perkuliahan.
11. Seluruh teman teman pengurus HIMATIFA UPN “Veteran” Jawa Timur periode 2020/2021, dan periode 2022/2023 yang telah menemani hari hari saya berkuliah, dan menemani proses perkembangan softskill saya selama perkuliahan.
12. Anggota grup CAMPSEGGSS, grup yang full drama, full canda tawa, full galau, full haha hihi.
13. Teman teman dekat saya. Dhany sang badut, Kepin sang badut 2, Galih raja mancing, Patur sang galau, Alpin sang penakluk wanita, Fros sang petarung, Dede sang penakluk wanita 2, Dio pemilik djarum, Abi sang nmax, Aan penguasa angkringan.
14. Seluruh teman teman Angkatan 2019 Informatika UPN Veteran Jawa Timur.
15. Wanita yang di pertemukan di akhir masa perkuliahan. FKPS, 06062001. Yang memberikan senyum, canda tawa, semangat, dan hal serupa kepada saya. Sehingga saya semakin berkobar kobar untuk menyelesaikan skripsi saya.
16. Semua pihak pihak yang bersinggungan kepada saya, yang tidak dapat saya sebutkan satu persatu.

Semoga Tuhan Yang Maha Esa memberikan balasan yang berlipat ganda atas kebaikan yang diberikan.

Surabaya, 20 November 2023

Penulis,



Nico Natanael

NPM. 19081010023

DAFTAR ISI

BAB I PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Rumusan Masalah 4

1.3. Tujuan 4

1.4. Manfaat 4

1.5. Batasan Masalah 5

BAB II TINJAUAN PUSTAKA 6

2.1. Penelitian Sebelumnya 6

2.2. Landasan Teori 8

2.2.1. Black Box 8

2.2.2. White Box 8

2.2.3. Grey Box 9

2.2.4. Website 10

2.2.5. Domain 11

2.2.6. Alamat IP 13

2.2.7. Web Direktori 13

2.2.8. Google Dorking 14

2.2.9. Server Website 15

2.2.10. Cyber Security(CIA TRIAD) 16

2.2.11. Vulnerability Assesment 19

2.2.12. Penetration Testing 19

2.2.13. OWASP 20

2.2.14. OWASP Top 10 21

2.2.15. Vulnerability Scanning Tools 24

2.2.12.1.Nessus 25

2.2.12.2. OWASP ZAP 26

2.2.12.3. NMAP 27

2.2.12.4. Nslookup 28

2.2.12.5. Whoami 28

2.2.12.6. Whatweb 29

BAB III METODOLOGI 31

3.1. Lokasi Penelitian 31

3.2. Objek Penelitian 31

3.3. Alat Penelitian 31

3.3.1. Perangkat Keras 31

3.3.2. Perangkat Lunak 32

3.4. Bahan Penelitian 34

3.5. Metode Pengumpulan Data 34

3.5.1. Metode Observasi 34

3.5.2. Metode Studi Kepustakaan 34

3.6. Langkah Penelitian 35

3.6.1. Pre-engagement Interactions 36

3.6.1.1. Scoping 36

3.6.1.2. Consent 36

3.6.1.3. Information Gathering 36

3.6.2. Intelegence Gathering 37

3.6.2.1. REVERSE IP DOMAIN CHECK 38

3.6.2.2. NETWORK RANGE USING ARIN 38

3.6.2.3. PING 38
3.6.2.4. NSLOOKUP 39
3.6.2.5. WHOIS 40
3.6.2.6. NMAP 40
3.6.3. Vulnerability Testing 41
3.6.3.1. Nessus 41
3.6.3.2. NMAP Dengan Script Vulscan 42
3.6.3.3. OWASP ZAP 43
3.6.4. Exploitation 44
3.6.5. Reporting 45
3.6.6. Rekomendasi 52
BAB IV HASIL DAN PEMBAHASAN 53
4.1. Pre-Engagement Interaction 53
4.1.1. Scope 53
4.1.2. Consent 54
4.1.3. Information Gathering 54
4.1.3.1. Wappalyzer Website LPPM 54
4.1.3.2. Wappalyzer Website LP3M 55
4.1.3.3. Wappalyzer Website International Office 55
4.1.3.4. Wappalyzer Website PPID 56
4.1.3.5. Wappalyzer Website SIMARIS 56
4.1.3.6. WhatWeb Website LPPM 57
4.1.3.7. WhatWeb Website LP3M 58
4.1.3.8. WhatWeb Website PPID 59
4.1.3.9. WhatWeb Website International Office 60

4.1.3.10. WhatWeb Website SIMARIS 61
4.2. Intelegance Gathering 62
4.2.1. Reverse IP Domain Check 62
4.2.2. Network Range Using Arin 63
4.2.3. Ping 65
4.2.3.1. Ping Standar 66
4.2.3.2. Ping Menghitung Maximum Frame Size 66
4.2.3.3. Ping Mngetahui Total Hop 68
4.2.4. Nslookup 70
4.2.5. Whois 72
4.2.6. Nmap 73
4.2.6.1. Perform TCP Connect 73
4.2.6.2. Perform UDP Scan 74
4.2.6.3. Perform Service Version Discovery 74
4.3. Vulnerability Testing 75
4.3.1. Nessus Terhadap Website LPPM 75
4.3.2. Nessus Terhadap Website LP3M 77
4.3.3. Nessus Terhadap Website International Office 78
4.3.4. Nessus Terhadap Website PPID 79
4.3.5. OWASP ZAP Terhadap Website LPPM 81
4.3.6. OWASP ZAP Terhadap Website LP3M 82
4.3.7. OWASP ZAP Terhadap Website International Office 82
4.3.8. OWASP ZAP Terhadap Website PPID 83
4.3.9. OWASP ZAP Terhadap Website SIMARIS 84
4.3.10. NMAP Script Vulscan 85

4.4. Exploitation 91
4.4.1. Website LPPM_Path Traversal 91
4.4.2. Website LPPM_SQL Injection - SQLite 94
4.4.3. Website LPPM_.htaccess Information Leak 96
4.4.4. Website LPPM_ Application Error Disclosure 97
4.4.5. Website LPPM_DDoS Attack 99
4.4.6. Website International Office_ Path Traversal 100
4.4.7. Website International Office_ SQL Injection 103
4.4.8. Website International Office_ web.config File Information Disclosure 104
4.4.9. Website International Office_DDoS Attack 105
4.4.10. Website PPID_ Browsable Web Directories 106
4.4.11. Website PPID_ Server Side Template Injection (Blind) 107
4.4.12. Website PPID_Remote OS Command Injection 108
4.4.13. Website PPID_DDoS Attack 109
4.4.14. Website SIMARIS_Hidden File Found 110
4.4.15. Website SIMARIS_Directory Browsing 110
4.4.16. Website SIMARIS_Application Error Disclosure 112
4.4.17. Website SIMARIS_DDoS Attack 113
4.4.18. Website LP3M_DDoS Attack 114
4.5. Reporting 115
4.5.1. Website PPID 115
4.5.1.1. Hasil Peringatan 117
4.5.1.2. Hasil Perhitungan CVSS 120
4.5.2. Website LP3M 121
4.5.2.1. Hasil Peringatan 122

4.5.2.2. Hasil Perhitungan CVSS 124
4.5.3. Website LPPM 126
4.5.3.1. Hasil Peringatan 127
4.5.3.2. Hasil Perhitungan CVSS 128
4.5.4. Website International Office 130
4.5.4.1. Hasil Peringatan 131
4.5.4.2. Hasil Perhitungan CVSS 133
4.5.5. Website SIMARIS 134
4.5.5.1. Hasil Peringatan 135
4.5.5.2. Hasil Perhitungan CVSS 137
4.6. Rekomendasi 138
4.6.1. Website PPID_ Browsable Web Directories 138
4.6.2. Website PPID_ Server Side Template Injection (Blind) 139
4.6.3. Website PPID_Remote OS Command Injection 140
4.6.4. Website PPID_DDoS Attack 141
4.6.5. Website LPPM_Path Traversal 142
4.6.6. Website LPPM_SQL Injection – SQLite 144
4.6.7. Website LPPM_.htaccess Information Leak 145
4.6.8. Website LPPM_ Application Error Disclosure 146
4.6.9. Website LPPM_DDoS Attack 147
4.6.10. Website International Office_ Path Traversal 148
4.6.11. Website International Office_ SQL Injection 150
4.6.12. Website International Office_ web.config File Information Disclosure 151
4.6.13. Website International Office_DDoS Attack 152
4.6.14. Website SIMARIS_Hidden File Found 153

4.6.15. Website SIMARIS_Directory Browsing 153

4.6.16. Website SIMARIS_Application Error Disclosure 154

4.6.17. Website SIMARIS _DDoS Attack 156

4.6.18. Website LP3M_DDoS Attack 157

BAB V KESIMPULAN DAN SARAN 159

5.1. Kesimpulan 159

5.2. Saran 160

DAFTAR PUSTAKA 161

DAFTAR GAMBAR

Gambar 1. 1 OWASP TOP 10 : 2021 3
Gambar 2. 1 CIA TRIAD 17
Gambar 2. 2 Perbandingan OWASP TOP 10 Tahun 2021 dengan 2017 22
Gambar 2. 3 Nessus Vulnerability Scanner 25
Gambar 2. 4 OWASP Zed Attack Proxy 26
Gambar 2. 5 NMAP 27
Gambar 3. 1 Diagram Alir Penelitian 35
Gambar 3. 2 Diagram Alir information Gathering 36
Gambar 3. 3 Diagram Alir Intelegence Gathering 37
Gambar 3. 4 Diagram Alir Reverse IP Domain Check 38
Gambar 3. 5 Diagram Alir Arin 38
Gambar 3. 6 Diagram Alir Ping 38
Gambar 3. 7 Diagram Alir Nslookup 39
Gambar 3. 8 Diagram Alir Whois 40
Gambar 3. 9 Diagram Alir NMAP 40
Gambar 3. 10 Tampilan Nessus 41
Gambar 3. 11 Tampilan Web Application Test Nessus 41
Gambar 3. 12 Logo Vulscan.NSE 42
Gambar 3. 13 Tampilan OWASP ZAP 43
Gambar 3. 14 Tampilan Manual Explore OWASP ZAP 43
Gambar 3. 15 Hasil Scan Pada Kolom Alert 44
Gambar 3. 16 Fitur Intercept Burpsuite 44
Gambar 3. 17 Fitur Repeater Burpsuite 45
Gambar 4. 1 Wappalyzer_LPPM 54
Gambar 4. 2 Wapplyzer_LP3M 55
Gambar 4. 3 Wapplyzer_IO 55
Gambar 4. 4 Wappalyzer_PPID 56
Gambar 4. 5 Wappalyzer_SIMARIS 56
Gambar 4. 6 Hasil Whatweb LPPM 57
Gambar 4. 7 Hasil Whatweb LP3M 58
Gambar 4. 8 Hasil Whatweb PPID 59
Gambar 4. 9 Hasil Whatweb IO 60

Gambar 4. 10 Hasil Whatweb SIMARIS.....61
Gambar 4. 11 Hasil Reverse IP Domain Check.....62
Gambar 4. 12 Dashboard Arin.....63
Gambar 4. 13 Hasil Arin_1.....64
Gambar 4. 14 Hasil Arin_2.....64
Gambar 4. 15 Hasil Arin_3.....65
Gambar 4. 16 Hasil Ping Standar.....66
Gambar 4. 17 Hasil Pencarian Maximum Frame Size_1.....67
Gambar 4. 18 Hasil Pencarian Maximum Frame Size_2.....67
Gambar 4. 19 Hasil Pencarian Maximum Frame Size_3.....68
Gambar 4. 20 Hasil Pencarian Maximum Frame Size_4.....68
Gambar 4. 21 Hasil Pencarian Total Hop_1.....69
Gambar 4. 22 Hasil Pencarian Total Hop_2.....69
Gambar 4. 23 Hasil Pencarian Total Hop_3.....70
Gambar 4. 24 Tampilan nslookup.....70
Gambar 4. 25 Identitas Server.....71
Gambar 4. 26 IP Address Server.....71
Gambar 4. 27 Hasil Scan Dengan Whois.....72
Gambar 4. 28 Hasil TCP Scan.....73
Gambar 4. 29 Hasil TCP Scan.....73
Gambar 4. 30 Hasil Scan UDP.....74
Gambar 4. 31 Hasil Scan Service Version Discovery.....74
Gambar 4. 32 Hasil Scanning LPPM Dengan Nessus.....75
Gambar 4. 33 Host Information.....76
Gambar 4. 34 Vulnerabilites LPPM Dengan Nessus.....76
Gambar 4. 35 Hasil Scanning LP3M Dengan Nessus.....77
Gambar 4. 36 Host Information LP3M.....77
Gambar 4. 37 Vulnerabilities LP3M Dengan Nessus.....77
Gambar 4. 38 Hasil Scanning IO dengan Nessus.....78
Gambar 4. 39 Host Information IO.....78
Gambar 4. 40 Host Information IO.....78
Gambar 4. 41 Vulnerabilities LP3M Dengan Nessus.....78
Gambar 4. 42 Hasil Scanning PPID dengan Nessus.....79
Gambar 4. 43 Host Information PPID.....79

Gambar 4. 44 Vulnerabilites PPID dengan Nessus 80
Gambar 4. 45 Hasil Scanning LPPM dengan OWASP ZAP.....81
Gambar 4. 46 Hasil Scanning LP3M Dengan OWASP ZAP 82
Gambar 4. 47 Hasil Scanning OWASP ZAP_IO.....82
Gambar 4. 48 Hasil Scanning Website PPID Dengan OWASP ZAP.....83
Gambar 4. 49 Hasil Scanning Website SIMARIS Dengan OWASP ZAP 84
Gambar 4. 50 Path Traversal LPPM dengan OWASP ZAP.....91
Gambar 4. 51 Burpsuite Request dan Response Header.....91
Gambar 4. 52 Burpsuite Request dan Response Header_2.....92
Gambar 4. 53 Penyerangan Menggunakan Intruder Brupsuite.....92
Gambar 4. 54 Payloads Path Traversal.....93
Gambar 4. 55 Hasil Bruteforce Attack 93
Gambar 4. 56 Google Chrome Path Traversal LPPM 94
Gambar 4. 57 Terdeteksi SQL Injection.....94
Gambar 4. 58 Response dan Request Header SQL Injection LPPM.....95
Gambar 4. 59 Percobaan Pada Google Chrome.....95
Gambar 4. 60 Intruder Burpsuite 95
Gambar 4. 61 Payloads SQL Injection - SQLite.....96
Gambar 4. 62 Hasil Penyerangan Brute Force SQL Injection - SQLite.....96
Gambar 4. 63 .htaccess LPPM.....96
Gambar 4. 64 Request Header .htaccess LPPM 97
Gambar 4. 65 Response Header .htaccess LPPM.....97
Gambar 4. 66 Application Error Disclosure LPPM.....97
Gambar 4. 67 PHP Error LPPM 98
Gambar 4. 68 PHP Error LPPM_2 98
Gambar 4. 69 Request dan Response Header Login Website LPPM.....98
Gambar 4. 70 Penyerangan DDoS Menggunakan Kali Linux.....99
Gambar 4. 71 Ping Untuk Pembuktian.....99
Gambar 4. 72 Path Traversal IO Oleh OWASP ZAP.....100
Gambar 4. 73 Response dan Request Header Embed IO.....100
Gambar 4. 74 Request dan Response Header Path Traversal IO.....101
Gambar 4. 75 Firmware International Office 101
Gambar 4. 76 Target Brute Force Attack.....101
Gambar 4. 77 Payloads Bruteforce Attack Path traversal.....102

Gambar 4. 78 Hasil Bruteforce Attack Path Traversal 102
Gambar 4. 79 Hasil SQL Injection Website IO 103
Gambar 4. 80 Perintah SQLMap 103
Gambar 4. 81 Terdeteksi web.config Pada Nessus 104
Gambar 4. 82 Hasil Web Config IO 104
Gambar 4. 83 Percobaan DDoS Menggunakan Kali Linux 105
Gambar 4. 84 Ping Untuk Pembuktian 105
Gambar 4. 85 Terdeteksi Directory Browsing Web PPID 106
Gambar 4. 86 Hasil Google Dorking Website PPID 106
Gambar 4. 87 Hasil URL Pada Google Chrome 107
Gambar 4. 88 Vulnerable Server Side Template Injection (Blind) 107
Gambar 4. 89 Request dan Response Header Server Side Template Injection 108
Gambar 4. 90 Vulnerable Remote OS Command Injection 108
Gambar 4. 91 Request dan Response Header Remote OS Command Injection 108
Gambar 4. 92 Percobaan DDoS Menggunakan Kali Linux 109
Gambar 4. 93 Ping Untuk Pembuktian 109
Gambar 4. 94 Hidden File Found Website SIMARIS 110
Gambar 4. 95 PHPINFO 110
Gambar 4. 96 Informasi Directory Browsing SIMARIS 110
Gambar 4. 97 Hasil Google Dorking SIMARIS 111
Gambar 4. 98 Hasil Directory Browsing SIMARIS 111
Gambar 4. 99 PHP Error SIMARIS 112
Gambar 4. 100 PHP Error SIMARIS_2 112
Gambar 4. 101 Percobaan DDoS Menggunakan Kali Linux 113
Gambar 4. 102 Ping Untuk Pembuktian 113
Gambar 4. 103 Percobaan DDoS Menggunakan Kali Linux 114
Gambar 4. 104 Ping Untuk Pembuktian 114
Gambar 4. 105 Hasil DDoS LP3M 115
Gambar 4. 106 Hasil Akhir CVSS_PPID 121
Gambar 4. 107 Hasil Akhir CVSS_LP3M 125
Gambar 4. 108 Hasil Akhir CVSS_LPPM 130
Gambar 4. 109 Hasil Akhir CVSS_IO 134
Gambar 4. 110 Hasil CVSS_SIMARIS 138

DAFTAR TABEL

Tabel 4. 1 Hasil Scope 53
Tabel 4. 2 Hasil TCP Scan.....73
Tabel 4. 3 Hasil Scanning NMAP Vulscan 90
Tabel 4. 4 Alerts Counts_PPID.....117
Tabel 4. 5 Alerts Counts_LP3M 122
Tabel 4. 6 Alerts Count LPPM 126
Tabel 4. 7 Alerts Counts_IO 131
Tabel 4. 8 Alerts Counts_SIMARIS 135