Application Server Security Report

Period: 2016-05-26 to 2016-06-13

Generated At: 2016-06-14 17:09:29

Application Server Domain/IP: Total

Purpose

1. Help to find risk quickly and provide information such as attack source, target, impact and solutions.

Contents

Security Overview

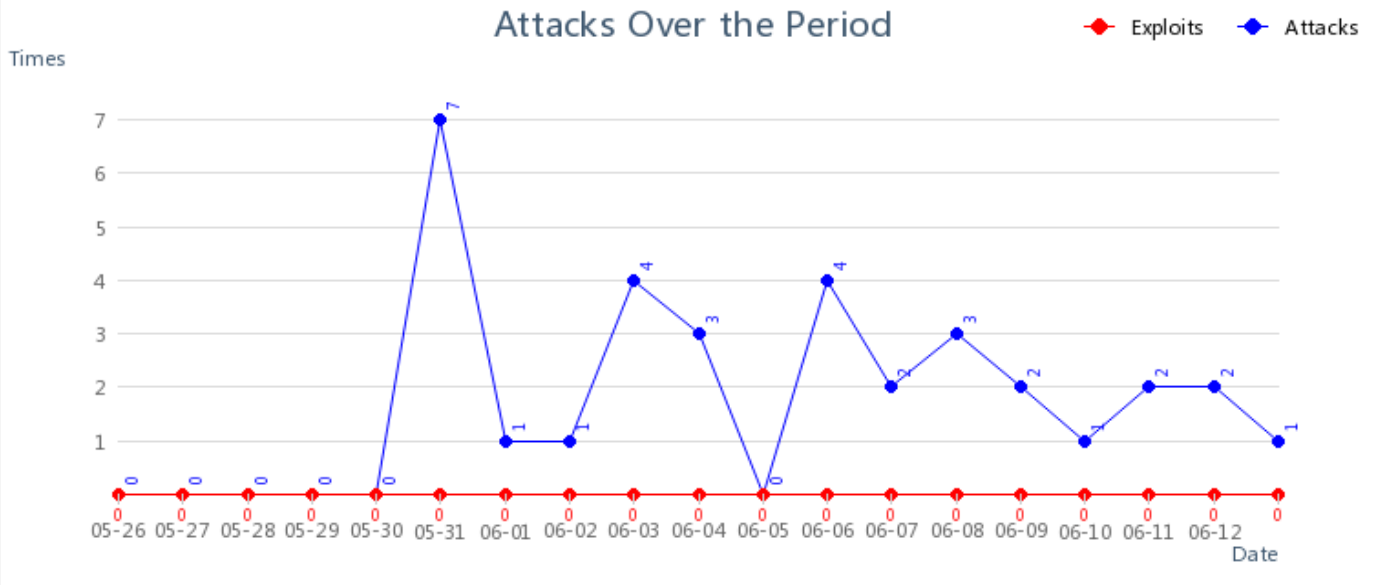
Summary

2016-05-26 to 2016-06-13, overall security rating is Fair, (see Security Rating Regulations).

After checking security of application servers based on Layer 2 to Layer 7 analysis, vulnerability analysis, License Detection, we found 4 Rule Database Expired, 0 high-risk vulnerabilities, average number of attacks each day is less than 100. Vulnerable targets are 216.58.196.33, 202.28.85.13, 216.58.196.193 Application Server Domain/IP,Application servers are undergoing few attacks, and the current protection policy can shield them away from eventual attack.

Attack possibility over the past period is as follows:

The more attacks, the worse the network security. The more exploits, the more likely the network will be intruded by attacker. Using next-generation firewall can protect the system against exploits and attacks by attackers. An exploit may be a piece of software that takes advantage of a bug or vulnerability in order to cause unintended behavior to computer software. And it's the attack that can be exploited by attackers, such as denial-of-service attack.



Security Rating

Security Rating Based on Attack

No.	Attack Type	Description	Attacks Per Day	Security Level
1	Application Server Security	Exploited but protected now	1	Good

Security Rating Based on Vulnerability

No.	Vulnerability Type	Description	High-Risk Vulnerabilities	Security Level
1	All Vulnerabilities	Potential risk	0	Excellent

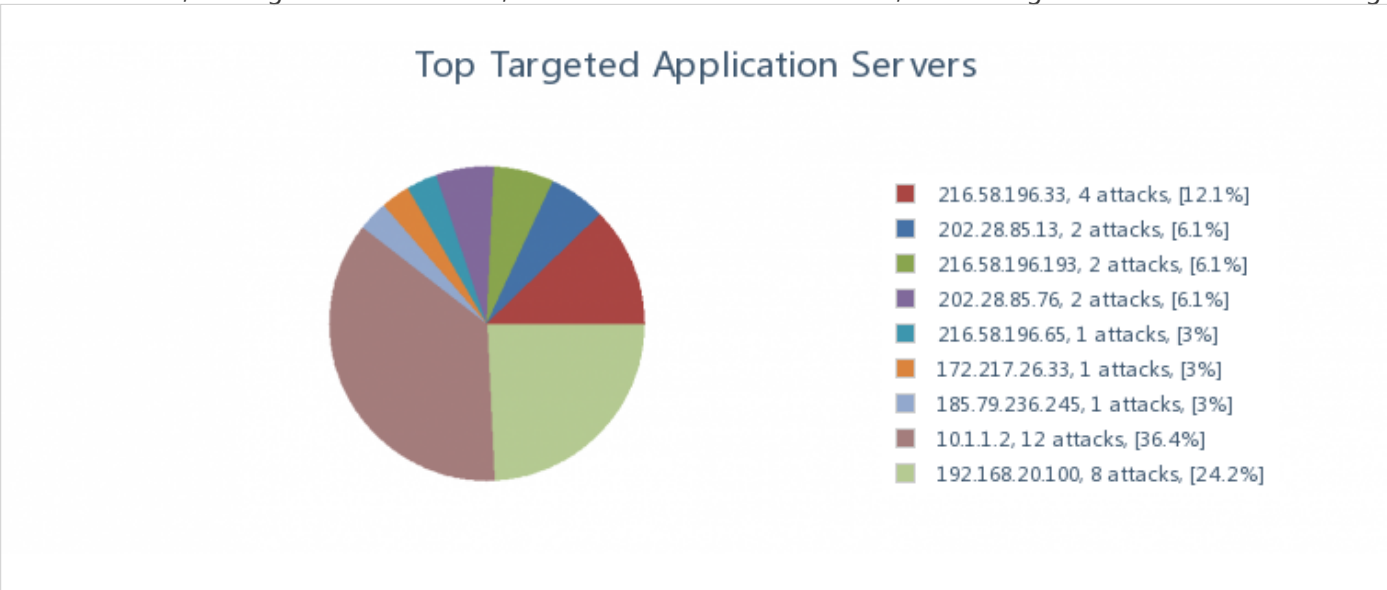
Security rating is based on rule event:

No.	Type	Description	Count	Security Level

1	Rule Database Detection	Vulnerability Database, WAF Signature Database, Anti-Virus Database, URL Database Rule Database Expired	4	Fair

Application Server Security

Application server 216.58.196.33 accounts for 12.12%, 202.28.85.13 accounts for 6.06%, 216.58.196.193 accounts for 6.06%, The higher the threat level, the more vulnerable the server is, and the higher threat the server is facing.



Attack Analysis

Top Targeted Application Servers

No.	Application Server	Attack Type	Attack Count	Percent	Exploits	Threat Level
1	216.58.196.33	UDP flooding attack(4)	4	12.12%	0	High
2	202.28.85.13	UDP flooding attack(2)	2	6.06%	0	High
3	216.58.196.193	UDP flooding attack(2)	2	6.06%	0	High
4	202.28.85.76	UDP flooding attack(2)	2	6.06%	0	High
5	216.58.196.65	UDP flooding attack(1)	1	3.03%	0	High
6	172.217.26.33	UDP flooding attack(1)	1	3.03%	0	High
7	185.79.236.245	UDP flooding attack(1)	1	3.03%	0	High
8	10.1.1.2	Port scan(12)	12	36.36%	0	Medium
9	192.168.20.100	Port scan(8)	8	24.24%	0	Medium

Most Vulnerable Application Servers

No.	Application Server	Vulnerability Type	Vulnerability Count	Exploits	Threat Level

No data available

Analysis Based on Risk Type

Based on analysis on traffic from several aspects, we found 2 categories of applications are in security threat. For those at high threat level, there are 1. For those at medium threat level, there are 1, which are as follows:

Application Server Security - Attack Types

No.	Attack Type	Attack Count	Percent	Exploited?	Threat Level
1	UDP flooding attack	13	39.4%	No	High
2	Port scan	20	60.6%	No	Medium

Application Server Security - Top Vulnerability Types

No.	Name	Vulnerability Count	Target IP	Threat Level

No data available

Analysis Based on Specific Attack

UDP Flooding Attack

Description

DDoS, Distributed Deny of Service in short, is an attack that attacker sends immense error data packets or partially connected packets to target server, with the purpose of consuming all the bandwidth and allowed connections, CPU and memory resources of the server, so that the server cannot provide services to legitimate users properly.

Target Server

UDP flooding attack: 13 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	216.58.196.33	-	4
2	202.28.85.13	-	2
3	202.28.85.76	-	2
4	216.58.196.193	-	2
5	172.217.26.33	-	1
6	216.58.196.65	-	1
7	185.79.236.245	-	1

Solution

1.Enable anti-DDoS attacks, both inside and outside DDoS attack, and configure the corresponding policy.

Port Scan

Description

DDoS, Distributed Deny of Service in short, is an attack that attacker sends immense error data packets or partially connected packets to target server, with the purpose of consuming all the bandwidth and allowed connections, CPU and memory resources of the server, so that the server cannot provide services to legitimate users properly.

Target Server

Port scan: 20 attacks, which are as follows:

No.	Target Domain/IP	Details	Attack Count
1	10.1.1.2	-	12
2	192.168.20.100	-	8

Solution

1.Enable anti-DDoS attacks, both inside and outside DDoS attack, and configure the corresponding policy.

Analysis Based on Specific Vulnerability

No data available

Security Rating

Excellent

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, no high-risk vulnerability is found. Threat does not affect application server security and user access right assignment. Critical security issue will not occur at present.

Good

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, less than 10 high-risk vulnerabilities are found. Average number of attacks each day is less than 100. Application server and user are undergoing few attacks, and the current protection policy can shield them away from eventual attack.

Fair

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, 10 - 50 high-risk vulnerabilities are found. Average number of attacks each day is between 100 and 1000. Application server and user are undergoing some attacks, and the current protection policy can shield them away from eventual attack.

Poor

After checking security of application servers and endpoint users based on Layer 2 to Layer 7 analysis and scanning, more than 50 high-risk vulnerabilities are found. Average number of attacks each day is more than 1000. Application server and user are undergoing a lot attacks, or even APT(Advanced Persistent Threat) attack. Urgent protection is needed and vulnerability must be fixed.

Remarks

When the device detects that license gets invalid, expired or the rule database license gets expired, the security rating will de degraded one rank; while APT or WebShell attack is detected, the security rating becomes critical.

Description

Current Software Version: AF6.8.232 EN Build20160328

Current Database Version:

No.	Name	Current Version Released
1	Anti-Virus Database	20160420 18:00:00
2	URL Database	20160523 09:00:00
3	Vulnerability Database	20160519 17:00:00
4	Software Update	20160407 15:19:00
5	Application Ident Database	20160516 12:34:56
6	WAF Signature Database	20160519 17:00:00
7	Data Leak Protection	20160519 20:18:08
8	Malware Signature Database	20160531 10:27:19
9	Vulnerability Analysis Rule	20160530 17:00:00
10	Malicious Connection Database	20160530 09:53:39
11	Threat Intelligence Database	20160506 12:30:01