ECR Security Assessment Report For:

SAMPLE

Revision History

Date	Version	Description	Author
5/17/2019	1	Final report	Brian Milliron

Table of Contents

Executive Summary

Between 5/16/19 and 5/17/19 Brian Milliron conducted a security assessment of 10 servers on the internal network, 10.0.0.0/24. Several serious vulnerabilities were identified which could compromise the confidentiality, availability, and integrity of the servers, and potentially create a foothold for further penetration into the enterprise.

Summary of Findings

Finding 1:	Vulnerable Webserver
Severity Level:	5
Disposition:	Open
Impact to Business:	Allows an attacker to create a new admin user

Finding 2:	Cleartext Passwords and PII Exposed
Severity Level:	5
Disposition:	Open
Impact to Business:	Allows an attacker to compromise other network hosts and sensitive data.

Finding 3:	SQL Injection
Severity Level:	4
Disposition:	Open
Impact to Business:	Allows an attacker to read and write data from the database without authenticating.

Finding 4:	Open Database Server
Severity Level:	4
Disposition:	Open
Impact to Business:	Allows an attacker to read data from the database without authenticating.

Finding 5:	Cleartext Login
Severity Level:	3
Disposition:	Open
Impact to Business:	Allows an attacker to capture logins

Finding 6:	Information Disclosure
Severity Level:	2
Disposition:	Open
Impact to Business:	Aids an attacker in gaining unauthorized access.

Vulnerability Severity Levels

	5	4	3	2	1
Number of Findings	2	2	1	1	0

Objective

The objective of the security assessment is to provide an assessment of the security posture of the targets that are discovered during the assessment period. This report helps by gauging issues found during the assessment against industry standards, corporate policy, and the knowledge of the assessors.

Assessment Scope

The security assessment was focused on internal network 10.0.0.0/24. No testing was done on the supporting infrastructure. The results from this test are not intended to be an assessment of all applications, or entire infrastructure, and pertain only of those targets identified within this assessment's scope. While changes to the infrastructure, application code, configurations and architectures may always be in progress, the assessment provided in this report only presents those issues which existed during the assessment period. Findings listed in this report are a snapshot of the issues discovered, which existed during the assessment period, and may not be current. Findings discussed in this document are representative of issues in general and may not list all instances of a specific issue. The assessment also did not perform any denial of service (DoS) attacks against the network, its subsystems, devices or applications in order to minimize the potential of interrupting operations.

Assessment Tools

A variety of automated and manual tools are used to increase the thoroughness of the analysis as well as to increase efficiency and promote the re-usability and standardization of components. The following list of tools are the most common that are used, but may not be all inclusive.

- Metasploit
- Sqlmap
- Nmap
- Impacket
- Burp
- Epowner
- Mongoextract
- Custom Scripts

Target Systems

This Assessment was conducted in the following environments:

- Production

The following IP Address(es) and/or URL's were assessed:

- 10.0.0.1
- 10.0.0.2
- 10.0.0.10 DC01.blustar.com
- 10.0.0.11
- 10.0.0.21
- 10.0.0.23 PRD03.blustar.com
- 10.0.0.26
- 10.0.0.186
- 10.0.0.229
- 10.0.0.247 PRD02.blustar.com

The following IP Address(es) and/or URL's were out of scope and were not assessed:

- 10.0.0.216 www.schellman.info

Security Assessment Results

Several commendable security features were noted by the assessor during testing. Usernames are randomized rather than based on the employees given name, making phishing attacks more difficult. Passwords are complex and would be difficult to brute force. Most of the servers have been hardened and/or updated, several of which are linux, which makes it more difficult for an attacker to find a foothold. There were no unnecessary ports found open.

Despite these positives, serious security flaws were uncovered which would allow a skilled attacker to compromise the entire network and possibly infiltrate deeper into other network segments. Only a single server is badly out of date on security updates, but that was enough to allow me to gain access to the domain controller. The cleartext userdata including passwords and PII are especially concerning, since they would allow an attacker to infiltrate the entire network, and the PII could expose the company to legal risk.

Recommendations

PRD02 presents a serious risk to other company assets because it can be used as a staging point to serve malware to the Mcafee AV clients configured to use it to pull updates. It is highly recommended to apply security fixes ASAP or retire it so it does not continue to present a threat to the rest of the company.

In addition to the suggested hotfixes, another recommendation would be to offer security awareness training to the developers to prevent security mistakes from occurring in the first place.

Severity 5 (Critical) Findings

Finding 1: Vulnerable Webserver

Asset(s) Affected: 10.0.0.247 [PRD02.blustar.com]

Issue: Mcafee EPO 4.6.4 is vulnerable to SQL Injection and Directory Traversal File Upload

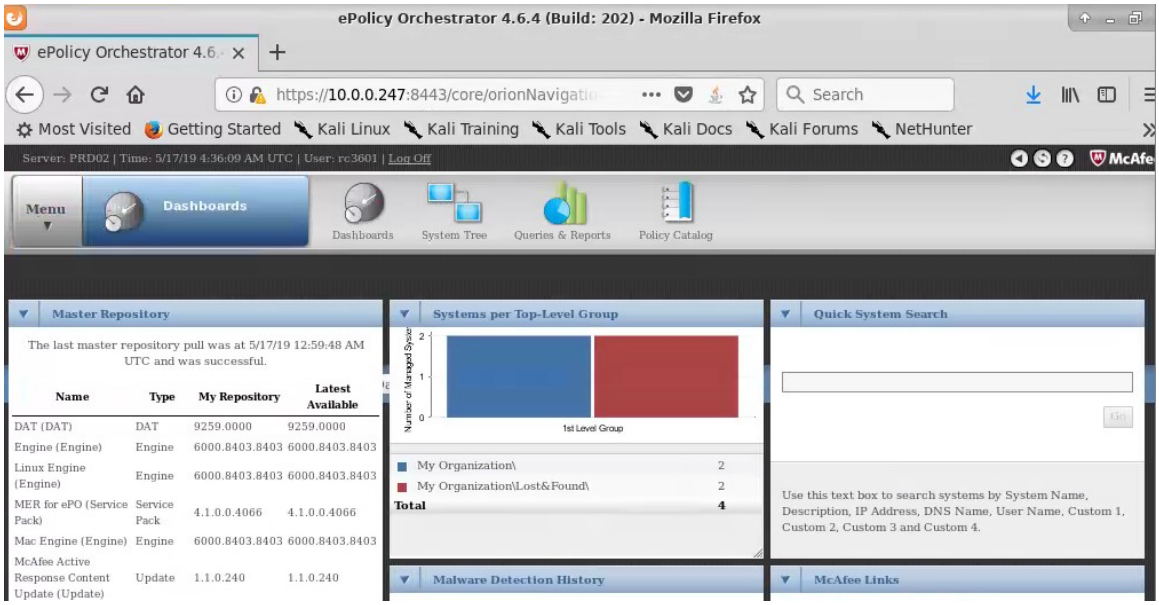
Description: This server hosts a Mcafee ePolicy Orchestrator (EPO) which is being used to manage the anti-virus clients for the subnet. However it is missing some critical system security patches and is well out of date. There are 2 related vulnerabilities in the webserver component of EPO, a SQL injection and a directory traversal/file upload vulnerability.

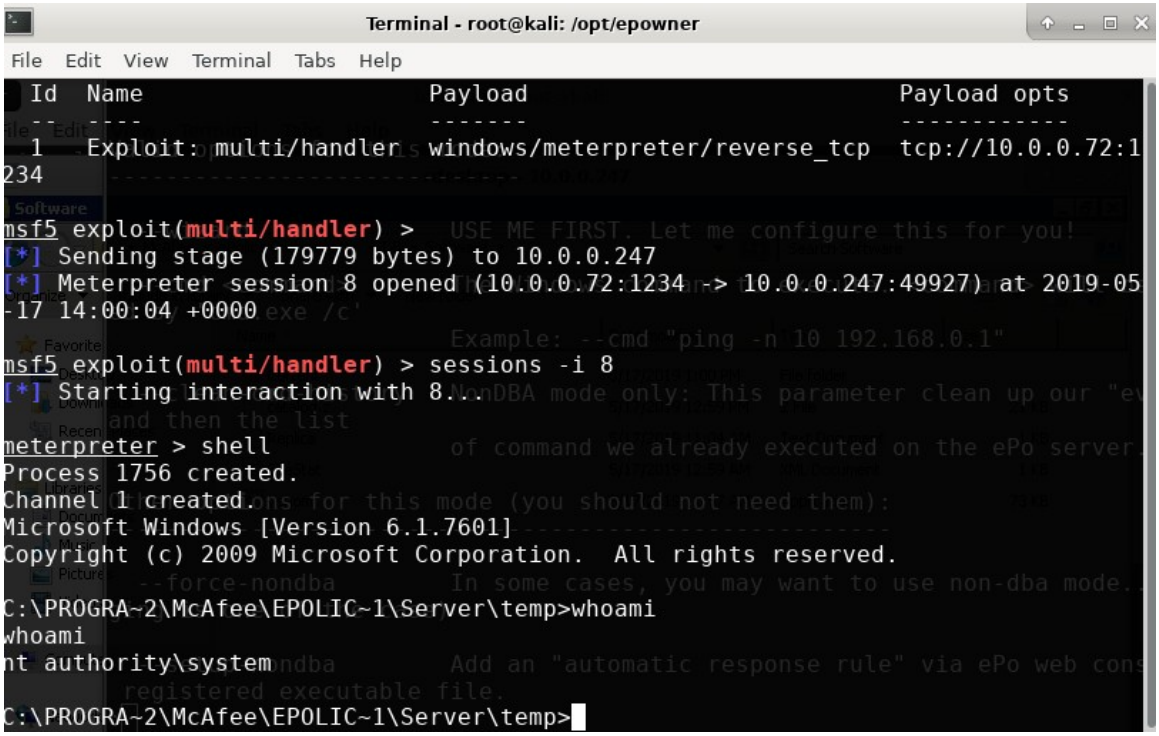
The SQL injection allows write access to the user database enabling me to write a new admin user which I can then use to alter the configuration settings of the application. The file upload directory traversal vulnerability allows uploading malware to the server, which can then be pushed out to clients in the form of a malicious “update”.

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.

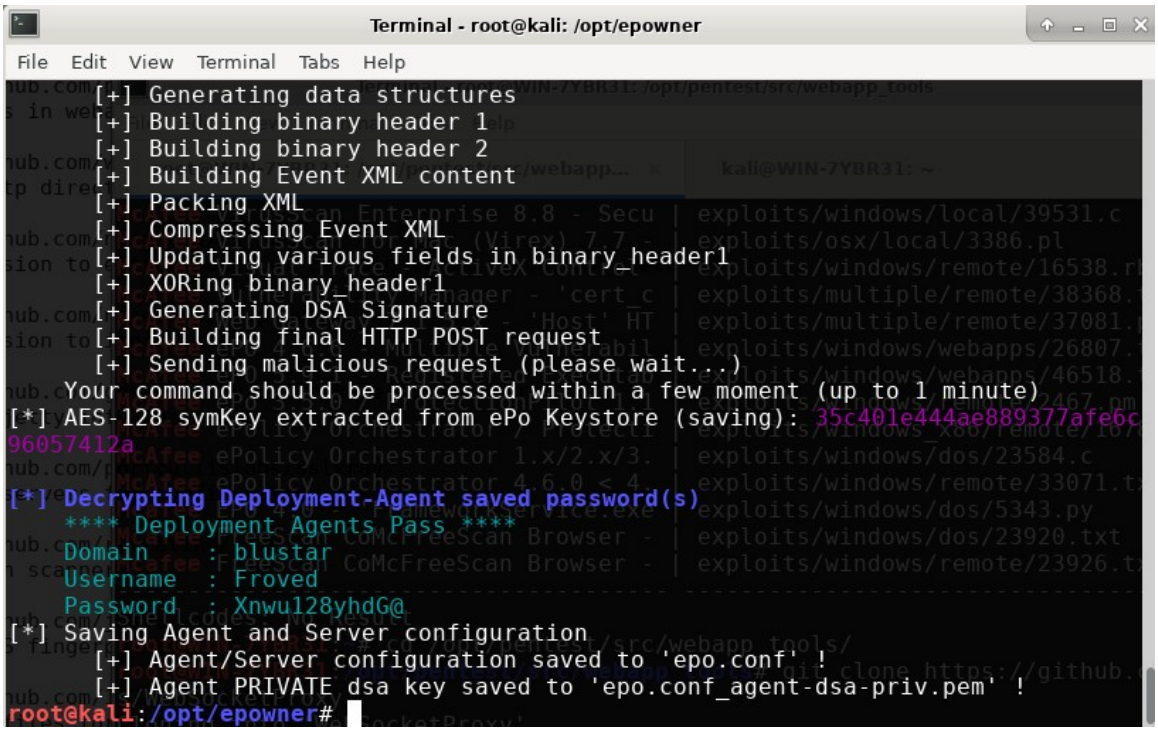
File path traversal vulnerabilities arise when user-controllable data is used within a filesystem operation in an unsafe manner. Typically, a user-supplied filename is appended to a directory prefix in order to read or write the contents of a file. If vulnerable, an attacker can supply path traversal sequences (using dot-dot-slash

characters) to break out of the intended directory and read or write files elsewhere on the filesystem.





I was able to leverage the new admin web account to exploit the OS and run malicious code in the SYSTEM security context, dump cleartext passwords from memory, and gain control of a highly privileged user account to move laterally in the network and gain access to the domain controller DC01.



Recommendations: Upgrade to 4.6.6 or newer.

References:

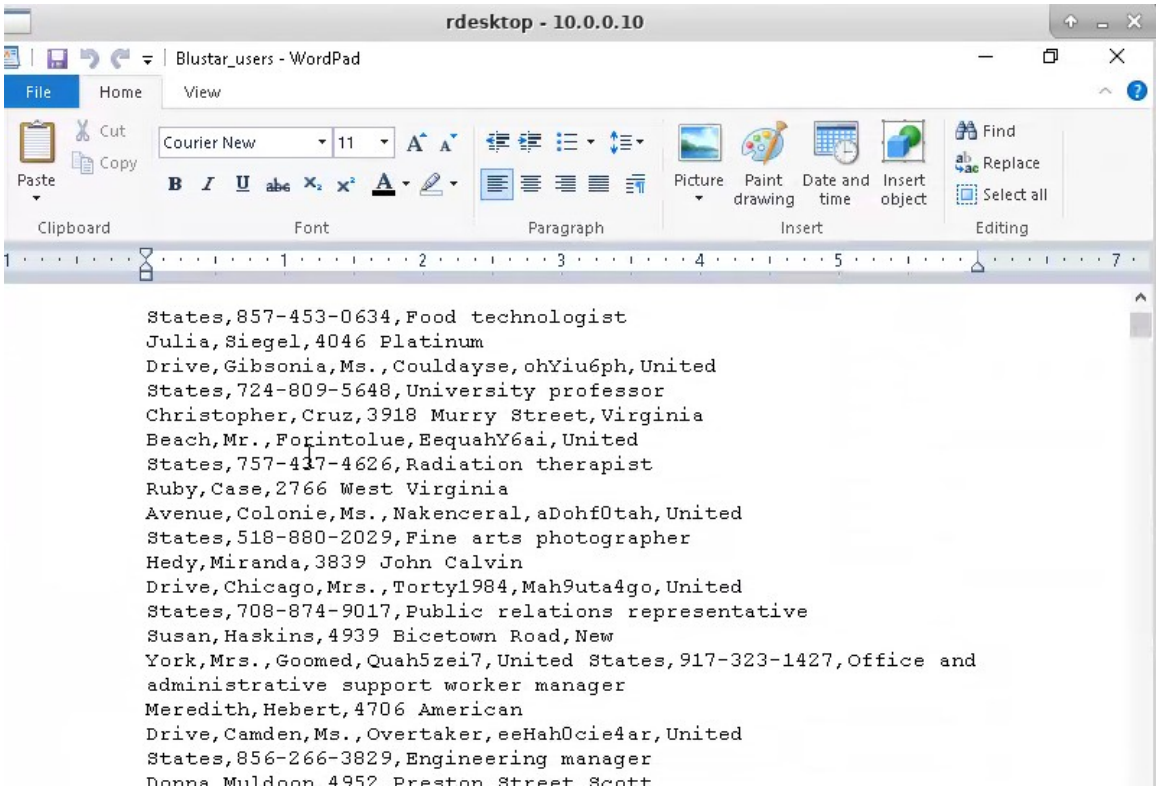
CVE-2013-0140
CVE-2013-0141

Finding 2: Cleartext Passwords and PII Exposed

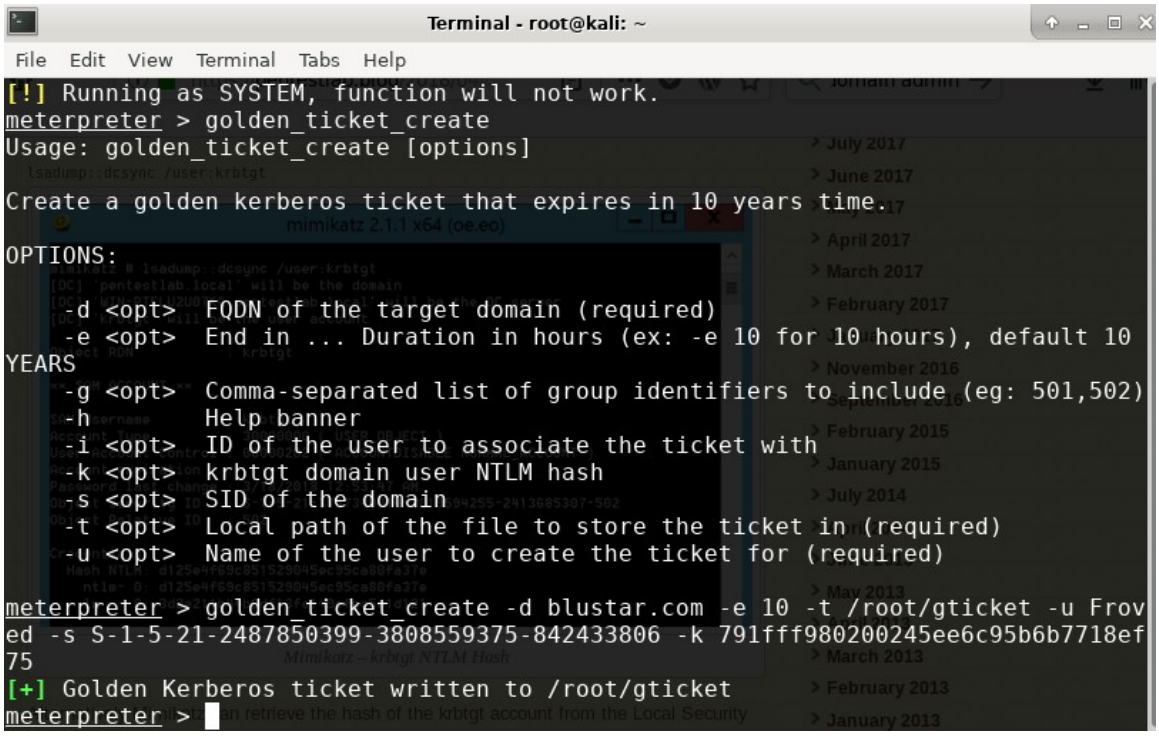
Asset(s) Affected: 10.0.0.10 [DC01.blustar.com]

Issue: An unencrypted text file containing a large amount of sensitve data was located on server DC01

Description: Using the account data from having compromised PRD02 I was able to RDP into domain controller DC01. I found some working data on the administrator's desktop. This data included full usernames, passwords, addresses, phone numbers, and social security numbers for more than 3000 employees.



Additionally I was able to extract user account data from the ntds.dit file and the SYSTEM hive to create a forged kerberos ticket granting ticket, also known as a golden ticket, which never expires and can be used to maintain access to the network even after the passwords have been changed. A malicious attacker could use this type of access to maintain a stealthy presence even after you think he is gone, maintaining persistent access for months or years.



Recommendations: Secure highly sensitive data such as SSNs and passwords using encryption.

References:
https://en.wikipedia.org/wiki/Encryption

Severity 4 (High) Findings

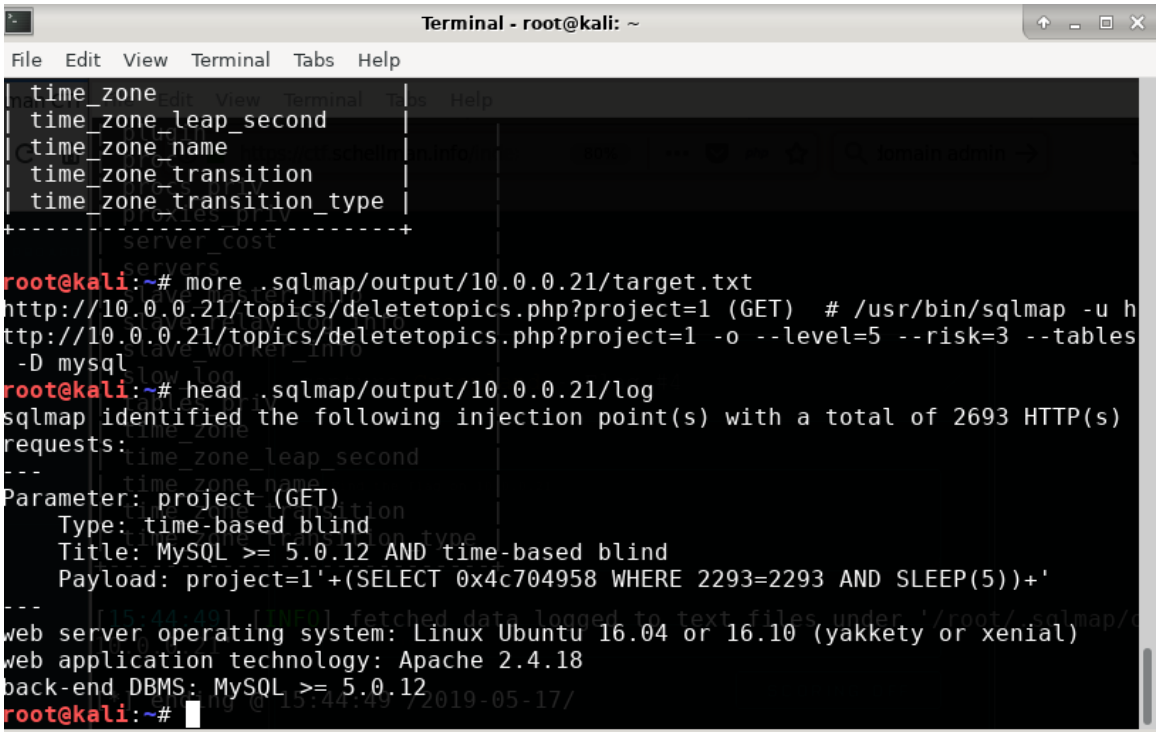
Finding 3: SQL Injection

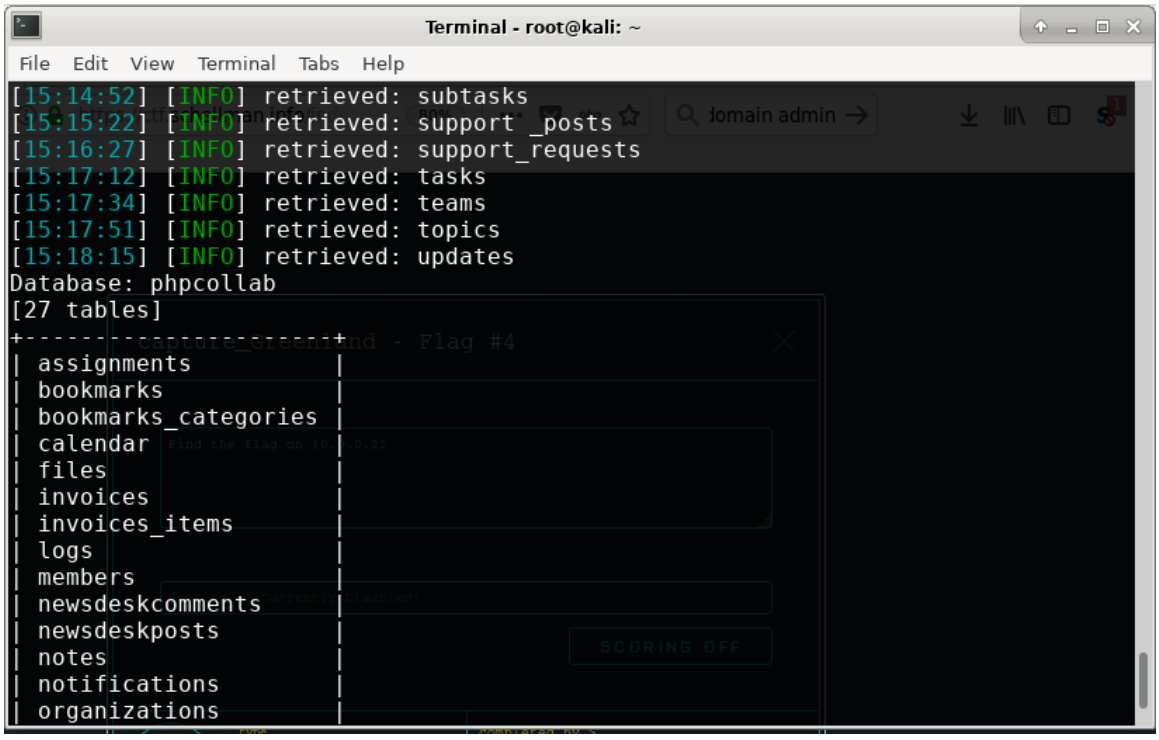
Asset(s) Affected: http://10.0.0.21/ [PhpCollab]

Issue: The project parameter on the login page [general/login.php] is vulnerable to SQL injection

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.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.





Recommendations: The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize every variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

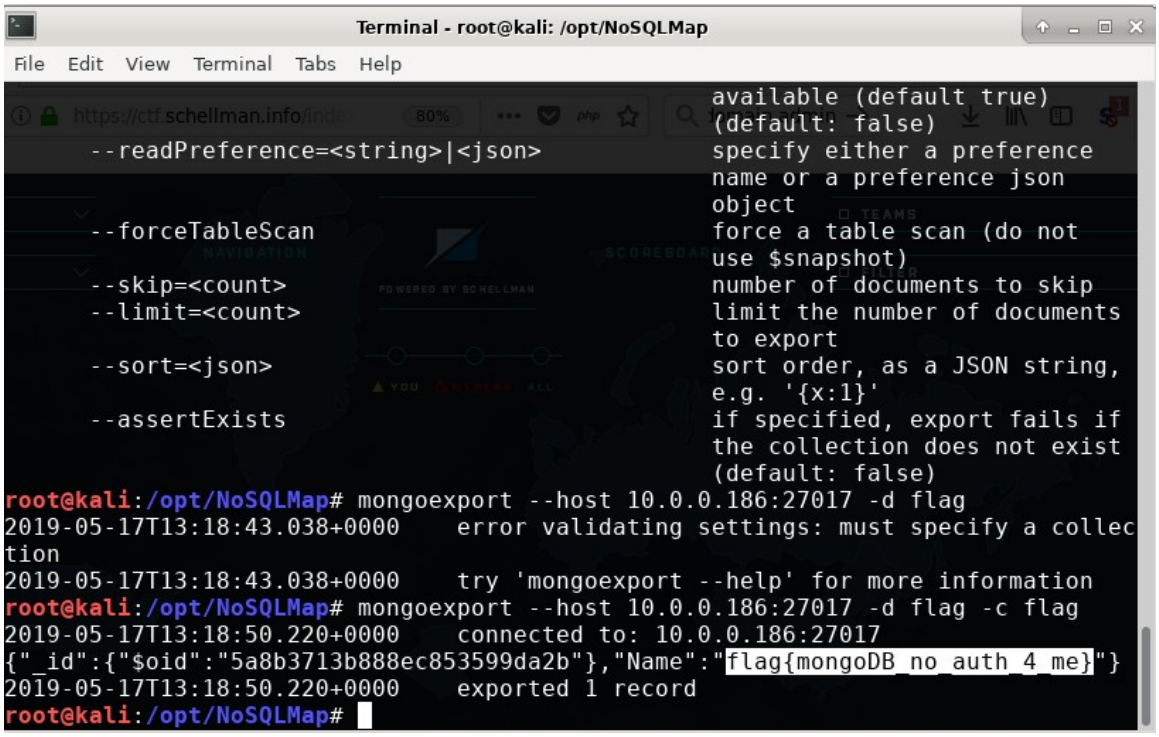
References:
https://en.wikipedia.org/wiki/SQL_injection
CVE-2017-6089

Finding 4: Open Database Server

Asset(s) Affected: 10.0.0.186

Issue: The server is hosting an unprotected mongo database on port 27017

Description: The mongo database on this server does not require any form of authentication and grants read access to everyone. A malicious user can steal sensitive data from the database.



Recommendations: Require a username and password so only authenticated and approved users can access the database.

Severity 3 (Medium) Findings

Finding 5: Cleartext Login

Asset(s) Affected: http://10.0.0.11, http://10.0.0.21, http://10.0.0.26:3000, http://10.0.0.229:8080

Issue: Several webservers allow login credentials to be transmitted over cleartext

Description: The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor the user login credentials in order to impersonate the user or gain unauthorized access to resources. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this.

Recommendations: Applications should use transport-level encryption (SSL/ TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

References:
https://en.wikipedia.org/wiki/Transport_Layer_Security

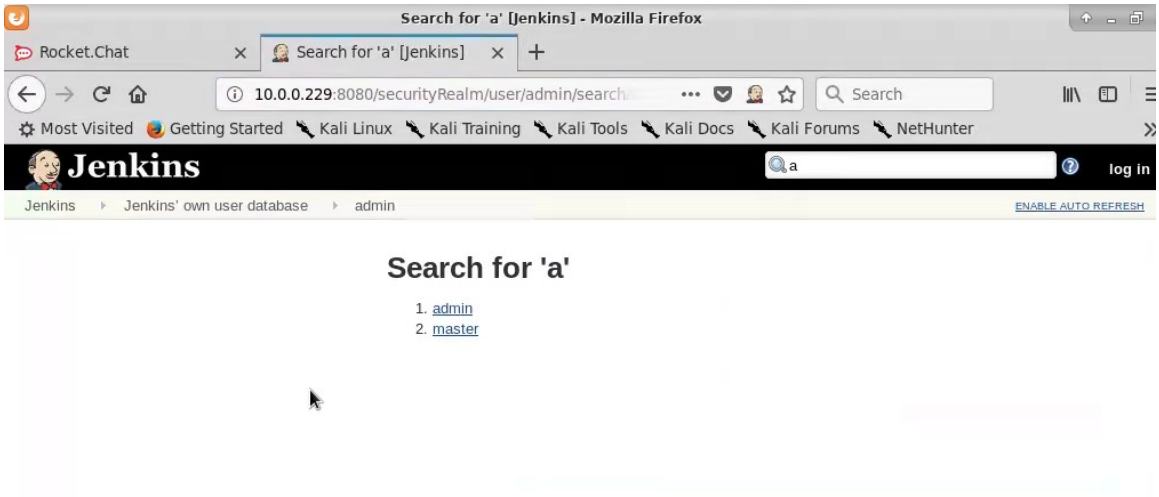
Severity 2 (Low) Findings

Finding 6: Information Disclosure

Asset(s) Affected: http://10.0.0.229:8080

Issue: The Jenkins web application allows unauthenticated users to display a list of application users.

Description: Any user who browses to this url http://10.0.0.229:8080/securityRealm/user/admin/search/index?q=a will be shown a list of users with the letter “a” in the name. By sequentially requesting a-z an attacker can gather a complete list of application users in order to launch a brute force password guessing attack and potentially gain unauthorized access to the Jenkins application.



Recommendations: Disable or restrict the search function to only authorized users.

References:
https://www.acunetix.com/vulnerabilities/web/jenkins-user-enumeration/

Vulnerability Classifications

Table Vulnerability Severity Scoring

Severity of Issue	Severity Level	Criteria	Mitigation Plan Date	Mitigate by Date
Critical	5	Serious and immediate threat to enterprise; confidentiality, integrity or availability of a critical resource could be compromised	n/a	Mitigation should commence immediately
High	4	Serious threat to application or critical resource	optional	0 – 4 weeks
Medium	3	Moderate threat to application or critical resource	2 weeks	0 – 8 weeks
Low	2	Minor threat to application or critical resource	4 weeks	4 – 24 weeks
Informational	1	General security information	n/a	n/a

Appendix A: Technical Data

Nmap Port Scan Results:

TCP Scan

Nmap scan report for 10.0.0.1

Host is up (0.00018s latency).

All 65535 scanned ports on 10.0.0.1 are filtered

MAC Address: 0A:74:B6:47:86:4A (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.18 ms 10.0.0.1

Nmap scan report for 10.0.0.2

Host is up (0.00030s latency).

Not shown: 65534 filtered ports

PORT STATE SERVICE VERSION

53/tcp open domain ISC BIND

MAC Address: 0A:74:B6:47:86:4A (Unknown)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|storage-misc|PBX

Running (JUST GUESSING): Linux 3.X (90%), HP embedded (89%), Vodavi embedded (87%)

OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/h:hp:p2000_g3 cpe:/h:vodavi:xts-ip

Aggressive OS guesses: Linux 3.8 (90%), HP P2000 G3 NAS device (89%), Vodavi XTS-IP PBX (87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.30 ms 10.0.0.2

Nmap scan report for 10.0.0.10

Host is up (0.00056s latency).

Not shown: 65515 filtered ports

PORT STATE SERVICE VERSION

53/tcp open domain?

| fingerprint-strings:

| DNSVersionBindReqTCP:

| version

|_ bind

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2019-05-16 22:23:59Z)

135/tcp open msrpc Microsoft Windows RPC

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: blustar.com, Site: Default-First-Site-Name)

445/tcp open microsoft-ds Windows Server 2016 Datacenter 14393 microsoft-ds (workgroup: BLUSTAR)

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: blustar.com, Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

3389/tcp open ms-wbt-server Microsoft Terminal Services

| ssl-cert: Subject: commonName=DC01.blustar.com

| Not valid before: 2019-05-14T15:13:25

|_Not valid after: 2019-11-13T15:13:25

|_ssl-date: 2019-05-16T22:26:14+00:00; -2s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

9389/tcp open mc-nmf .NET Message Framing

49668/tcp open msrpc Microsoft Windows RPC

49670/tcp open msrpc Microsoft Windows RPC

49671/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

49672/tcp open msrpc Microsoft Windows RPC

49683/tcp open msrpc Microsoft Windows RPC

49731/tcp open msrpc Microsoft Windows RPC

49782/tcp open msrpc Microsoft Windows RPC

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-TCP:V=7.70%I=7%D=5/16%Time=5CDDE306%P=x86_64-pc-linux-gnu%r(DNSV

SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\

SF:x04bind\0\0\x10\0\x03");

MAC Address: 0A:09:5D:E3:76:80 (Unknown)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2016|2012 (90%)

OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012

Aggressive OS guesses: Microsoft Windows Server 2016 (90%), Microsoft Windows Server 2012 (85%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (85%), Microsoft Windows Server 2012 R2 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: -1s, deviation: 2s, median: -2s

| smb-os-discovery:

| OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)

| Computer name: DC01

| NetBIOS computer name: DC01\x00

| Domain name: blustar.com

| Forest name: blustar.com

| FQDN: DC01.blustar.com

|_ System time: 2019-05-16T22:26:18+00:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: required

| smb2-security-mode:

| 2.02:

|_ Message signing enabled and required

| smb2-time:

| date: 2019-05-16 22:26:15

|_ start_date: 2019-05-15 15:13:29

TRACEROUTE

HOP RTT ADDRESS

1 0.56 ms 10.0.0.10

Nmap scan report for 10.0.0.11

Host is up (0.0068s latency).

Not shown: 65532 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)

```
| ssh-hostkey:
|   2048 a6:e7:57:1b:8c:29:12:99:95:95:b3:28:41:ce:9e:c3 (RSA)
|   256 29:41:54:a5:1f:d4:b7:df:7a:c9:f0:eb:2a:38:2b:39 (ECDSA)
|_  256 c3:6e:a8:50:aa:aa:1c:b9:69:30:db:e2:e3:0f:01:09 (ED25519)
80/tcp   open  http           Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
4000/tcp open  remoteanything?
MAC Address: 0A:D5:2C:1A:91:7A (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.13
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   6.83 ms 10.0.0.11



Nmap scan report for 10.0.0.21
Host is up (0.00069s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 79:5a:ee:98:93:ed:a9:18:48:41:7e:7d:48:59:85:28 (RSA)
|   256 c2:4c:c3:ec:7b:d3:79:bc:11:e2:5b:60:12:de:5f:e1 (ECDSA)
|_  256 f7:06:8a:39:d3:4c:90:13:5a:ab:e6:94:35:44:8c:e4 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

```
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: PhpCollab
|_Requested resource was general/login.php?PHPSESSID=uuhsbkn3oo5uvphp05kf234do6
MAC Address: 0A:FD:F0:80:ED:00 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.13
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 10.0.0.21

Nmap scan report for 10.0.0.23
Host is up (0.00045s latency).
Not shown: 65529 filtered ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=PRD03.blustar.com
| Not valid before: 2019-05-14T15:12:10
|_Not valid after:  2019-11-13T15:12:10
```

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49154/tcp open msrpc Microsoft Windows RPC

49167/tcp open msrpc Microsoft Windows RPC

MAC Address: 0A:49:B1:79:62:C0 (Unknown)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: -2s, deviation: 0s, median: -3s

| smb-security-mode:

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2019-05-16 23:12:30

|_ start_date: 2019-05-15 15:11:59

TRACEROUTE

```
HOP RTT     ADDRESS
1   0.45 ms 10.0.0.23


Nmap scan report for 10.0.0.26
Host is up (0.00089s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:15:9d:de:e6:d1:ee:98:03:b4:c9:7c:02:e5:69:33 (RSA)
|   256 f2:43:eb:e0:92:30:bc:05:c8:61:dc:cb:d9:c2:e3:51 (ECDSA)
|_  256 f0:b7:f1:7d:54:89:7f:b1:5f:02:4b:0f:d2:4b:5e:bc (ED25519)
3000/tcp open  ppp?
| fingerprint-strings:
|   DNSVersionBindReqTCP, Help, NCP, RPCCheck, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|   GetRequest:
|     HTTP/1.1 200 OK
|     X-Instance-ID: tT6TKCgEb4b5cFX5Z
|     Access-Control-Allow-Origin: *
|     Content-Type: text/html; charset=utf-8
|     set-cookie: connect.sid=s%3A4t7VDh3rDNOWH3tGk-WFExO41ad-
L57b.UD7TE0a7ws3GJFwB84PN5bK5d1ElW61jOyn8h%2BKcOyc; Path=/; HttpOnly
|     Vary: Accept-Encoding
|     Date: Thu, 16 May 2019 23:22:21 GMT
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <link rel="stylesheet" type="text/css" href="/theme.css?
371c471af472af9ebc733b4ae192407035e9da53">
|     <meta name="referrer" content="origin-when-cross-origin" />
```

| <script>/* eslint-disable */

| 'use strict';

| (function() {

| debounce = function debounce(func, wait, immediate) {

| timeout = void 0;

| return function () {

| _this = this;

| (var _len = arguments.length, args = Array(_len), _key = 0; _key < _len; _key++) {

| args[_key] = arguments[_key];

| later = function later() {

| timeout = null;

| !immedi

| HTTPOptions:

| HTTP/1.1 204 No Content

| X-Instance-ID: tT6TKCgEb4b5cFX5Z

| Access-Control-Allow-Origin: *

| Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE

| Vary: Access-Control-Request-Headers

| Content-Length: 0

| set-cookie: connect.sid=s
%3AhD12tomk_IvtqiLmDarpWvN4PVrsORTt.5Yh1uXaOYHQ8FoiG8n%2Fb
%2FnFjDykZGHQ5kktDqgZLjhE; Path=/; HttpOnly

| Date: Thu, 16 May 2019 23:22:22 GMT

|_ Connection: close

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port3000-TCP:V=7.70%I=7%D=5/16%Time=5CDDF0A9%P=x86_64-pc-linux-gnu%r(Ge

SF:tRequest,68DF,"HTTP/1\.1\x20200\x20OK\r\nX-Instance-ID:\x20tT6TKCgEb4b5

SF:cFX5Z\r\nAccess-Control-Allow-Origin:\x20*\r\nContent-Type:\x20text/ht

SF:ml;\x20charset=utf-8\r\nset-cookie:\x20connect\.sid=s%3A4t7VDh3rDNOWH3t

SF:Gk-WFExO41ad-L57b\.UD7TE0a7ws3GJFwB84PN5bK5d1ElW61jOyn8h%2BKcOyc;\
x20Pa

SF:th=/;\x20HttpOnly\r\nVary:\x20Accept-Encoding\r\nDate:\x20Thu,\x2016\x2

SF:0May\x202019\x2023:22:21\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYP

SF:E\x20html>\n<html>\n<head>\n<link\x20rel=\"stylesheet\"\x20type=\"text/

SF:css\"\x20href=\"/theme\.css\?371c471af472af9ebc733b4ae192407035e9da53\"

SF:>\n<meta\x20name=\"referrer\"\x20content=\"origin-when-cross-origin\"\x

SF:20/>\n<script>/*\x20eslint-disable\x20*/\n\n'use\x20strict';\n\(funct

SF:ion\(\)\x20{\n\tvar\x20debounce\x20=\x20function\x20debounce\(func,\x20

SF:wait,\x20immediate\)\x20{\n\t\tvar\x20timeout\x20=\x20void\x200;\n\t\tr

SF:eturn\x20function\x20\(\)\x20{\n\t\t\tvar\x20_this\x20=\x20this;\n\n\t\

SF:t\tfor\x20\(var\x20_len\x20=\x20arguments\.length,\x20args\x20=\x20Arra

SF:y\(_len\),\x20_key\x20=\x200;\x20_key\x20<\x20_len;\x20_key\+\+\)\x20{\

SF:n\t\t\t\targs\[_key\]\x20=\x20arguments\[_key\];\n\t\t\t}\n\n\t\t\tvar\

SF:x20later\x20=\x20function\x20later\(\)\x20{\n\t\t\t\ttimeout\x20=\x20nu

SF:ll;\n\t\t\t\t!immedi")%r(Help,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\

SF:n\r\n")%r(NCP,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(HTTPOp

SF:tions,18C,"HTTP/1\.1\x20204\x20No\x20Content\r\nX-Instance-ID:\x20tT6TK

SF:CgEb4b5cFX5Z\r\nAccess-Control-Allow-Origin:\x20*\r\nAccess-Control-Al

SF:low-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-Contr

SF:ol-Request-Headers\r\nContent-Length:\x200\r\nset-cookie:\x20connect\.s

SF:id=s%3AhD12tomk_IvtqiLmDarpWvN4PVrsORTt\.5Yh1uXaOYHQ8FoiG8n%2Fb
%2FnFjDy

SF:kZGHQ5kktDqgZLjhE;\x20Path=/;\x20HttpOnly\r\nDate:\x20Thu,\x2016\x20May

SF:\x202019\x2023:22:22\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPReq

SF:uest,1C,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(RPCCheck,1C,"HT

SF:TP/1\.1\x20400\x20Bad\x20Request\r\n\r\n")%r(DNSVersionBindReqTCP,1C,"H

SF:TTP/1\.1\x20400\x20Bad\x20Request\r\n\r\n");

MAC Address: 0A:45:4D:E3:73:E6 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.70%E=4%D=5/16%OT=22%CT=1%CU=30581%PV=Y%DS=1%DC=D
%G=Y%M=0A454D%T

OS:M=5CDDF0B5%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=107%TI=Z%CI=I
%II=I

OS:
%TS=8)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M
2301ST11N

OS:W7%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=68DF%W2=68DF%W3=68DF
%W4=68DF%W5=6

OS:8DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M2301NNSNW7%CC=Y
%Q=)T1(R=Y%DF=Y%T

OS:=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y
%T=40%W=0%S=A%A=Z%F=R

OS:%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
%RD=0%Q=)T6(R=Y%DF=Y%T=

OS:40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z
%A=S+%F=AR%O=%RD=0

OS:%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G
%RUCK=G%RUD=G)IE(R

OS:=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT ADDRESS

1 0.89 ms 10.0.0.26

Nmap scan report for 10.0.0.186

Host is up (0.00056s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol

2.0)

| ssh-hostkey:

| 2048 c4:e7:9c:eb:0b:f8:87:50:c5:44:bb:06:d5:b0:7e:05 (RSA)

```
|   256 14:c0:b5:65:b6:c2:83:8a:94:a7:53:9d:0f:f7:e3:7f (ECDSA)
|_  256 8f:f5:93:3d:e0:3e:65:5e:52:df:7a:81:57:86:d0:cb (ED25519)
27017/tcp open  mongodb MongoDB 3.6.2 3.6.2
| mongodb-databases:
|   ok = 1.0
|   databases
|     1
|       empty = false
|       sizeOnDisk = 12288.0
|       name = config
|     0
|       empty = false
|       sizeOnDisk = 32768.0
|       name = admin
|     3
|       empty = false
|       sizeOnDisk = 32768.0
|       name = jenkins
|     2
|       empty = false
|       sizeOnDisk = 32768.0
|       name = flag
|     4
|       empty = false
|       sizeOnDisk = 73728.0
|       name = local
|_  totalSize = 184320.0
| mongodb-info:
|   MongoDB Build info
|     maxBsonObjectSize = 16777216
|     ok = 1.0
```

| gitVersion = 489d177dbd0f0420a8ca04d39fd78d0a2c539420
| debug = false
| storageEngines
| 3 = wiredTiger
| 2 = mmapv1
| 1 = ephemeralForTest
| 0 = devnull
| modules
| javascriptEngine = mozjs
| bits = 64
| buildEnvironment
| distarch = x86_64
| ccflags = -fno-omit-frame-pointer -fno-strict-aliasing -ggdb -pthread -W
all -Wsign-compare -Wno-unknown-pragmas -Winvalid-pch -Werror -O2 -Wno-unused-lo
cal-typedefs -Wno-unused-function -Wno-deprecated-declarations -Wno-unused-but-s
et-variable -Wno-missing-braces -fstack-protector-strong -fno-builtin-memcmp
| cxx = /opt/mongodbtoolchain/v2/bin/g++: g++ (GCC) 5.4.0
| cc = /opt/mongodbtoolchain/v2/bin/gcc: gcc (GCC) 5.4.0
| linkflags = -pthread -Wl,-z,now -rdynamic -Wl,--fatal-warnings -fstack-p
rotector-strong -fuse-ld=gold -Wl,--build-id -Wl,--hash-style=gnu -Wl,-z,noexecs
tack -Wl,--warn-execstack -Wl,-z,relro
| target_arch = x86_64
| distmod = ubuntu1604
| target_os = linux
| cxxflags = -Woverloaded-virtual -Wno-maybe-uninitialized -std=c++14
| allocator = tcmalloc
| versionArray
| 3 = 0
| 2 = 2
| 1 = 6
| 0 = 3

```
|     version = 3.6.2
|     openssl
|       running = OpenSSL 1.0.2g  1 Mar 2016
|       compiled = OpenSSL 1.0.2g  1 Mar 2016
|     sysInfo = deprecated
|   Server status
|     uptimeMillis = 115943458
|     ok = 1.0
|     extra_info
|       page_faults = 251
|       note = fields vary by platform
|     connections
|       available = 51198
|       totalCreated = 6
|       current = 2
|     storageEngine
|       name = wiredTiger
|       persistent = true
|       supportsCommittedReads = true
|       readOnly = false
|         total_free_bytes = 2066744
|         pageheap_total_reserve_bytes = 71634944
|         thread_cache_free_bytes = 651984
|         pageheap_total_decommit_bytes = 38739968
|         max_total_thread_cache_bytes = 516947968
|         pageheap_reserve_count = 47
|         pageheap_scavenge_count = 81
|         pageheap_total_commit_bytes = 110276608
|         pageheap_unmapped_bytes = 98304
|         aggressive_memory_decommit = 0
|         pageheap_commit_count = 429
```

```
|     process = mongod
|     pid = 1164
|     version = 3.6.2
|     uptime = 115942.0
|_    host = ip-10-0-0-186
MAC Address: 0A:29:7A:A8:BB:32 (Unknown)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.13
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms 10.0.0.186

Nmap scan report for 10.0.0.216
Host is up (0.00057s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:1a:e6:b5:f6:0b:b9:d5:dd:1c:be:02:06:25:79:82 (RSA)
|   256 2a:e1:45:eb:22:aa:a6:5e:6d:10:12:37:3b:7b:50:2f (ECDSA)
|_  256 4f:f3:60:14:78:6c:c0:a9:61:30:54:a4:59:06:68:46 (ED25519)
80/tcp   open  http     nginx
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://10.0.0.216/
443/tcp  open  ssl/http nginx
|_http-server-header: nginx
```

|_http-title: Schellman CTF

| ssl-cert: Subject: commonName=*.schellman.info

| Subject Alternative Name: DNS:*.schellman.info, DNS:schellman.info

| Not valid before: 2018-12-18T15:39:25

|_Not valid after: 2020-02-16T15:29:02

|_ssl-date: TLS randomness does not represent time

| tls-alpn:

|_ http/1.1

| tls-nextprotoneg:

|_ http/1.1

5000/tcp open ssl/http Tornado httpd 4.5.3

|_http-server-header: TornadoServer/4.5.3

| http-title: CTF Maintenance

|_Requested resource was https://10.0.0.216:5000/index.html

| ssl-cert: Subject: commonName=*.schellman.info

| Subject Alternative Name: DNS:*.schellman.info, DNS:schellman.info

| Not valid before: 2018-12-18T15:39:25

|_Not valid after: 2020-02-16T15:29:02

|_ssl-date: TLS randomness does not represent time

MAC Address: 0A:71:65:F9:C1:F0 (Unknown)

Device type: general purpose

Running: Linux 3.X

OS CPE: cpe:/o:linux:linux_kernel:3

OS details: Linux 3.10 - 3.13

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT   ADDRESS

1   0.57 ms 10.0.0.216

Nmap scan report for 10.0.0.229

Host is up (0.00040s latency).

Not shown: 65527 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: BLUSTAR)

3389/tcp open ms-wbt-server Microsoft Terminal Service

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

8080/tcp open http Jetty 9.4.z-SNAPSHOT

8081/tcp open tcpwrapped

49158/tcp open msrpc Microsoft Windows RPC

Nmap scan report for 10.0.0.247

Host is up (0.0010s latency).

Not shown: 65517 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd

|_http-server-header: Apache

|_http-title: 403 Forbidden

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

443/tcp open ssl/https?

|_ssl-date: 2019-05-16T23:38:36+00:00; -3s from scanner time.

445/tcp open microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-ds

3389/tcp open ms-wbt-server Microsoft Terminal Service

|_ssl-date: 2019-05-16T23:38:37+00:00; -3s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

8081/tcp open tcpwrapped

8443/tcp open ssl/https-alt?

|_ssl-date: 2019-05-16T23:38:38+00:00; -3s from scanner time.

8444/tcp open ssl/pcsync-http?

|_ssl-date: 2019-05-16T23:38:36+00:00; -3s from scanner time.

47001/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49152/tcp open msrpc   Microsoft Windows RPC

49153/tcp open msrpc   Microsoft Windows RPC

49154/tcp open msrpc   Microsoft Windows RPC

49167/tcp open msrpc   Microsoft Windows RPC

49184/tcp open msrpc   Microsoft Windows RPC

49185/tcp open msrpc   Microsoft Windows RPC

49231/tcp open ms-sql-s   Microsoft SQL Server 2005 9.00.4035.00; SP3

| ms-sql-ntlm-info:

| Target_Name: BLUSTAR

| NetBIOS_Domain_Name: BLUSTAR

| NetBIOS_Computer_Name: PRD02

| DNS_Domain_Name: blustar.com

| DNS_Computer_Name: PRD02.blustar.com

| DNS_Tree_Name: blustar.com

|_ Product_Version: 6.1.7601

| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback

| Not valid before: 2019-05-15T15:12:31

|_Not valid after: 2049-05-15T15:12:31

|_ssl-date: 2019-05-16T23:38:35+00:00; -3s from scanner time.

MAC Address: 0A:83:D4:26:3C:22 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=7.70%E=4%D=5/16%OT=80%CT=1%CU=31305%PV=Y%DS=1%DC=D
%G=Y%M=0A83D4%T

OS:M=5CDDF5AA%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=104%TI=I%CI=I
%II=I

OS:%SS=S
%TS=7)OPS(O1=M2301NW8ST11%O2=M2301NW8ST11%O3=M2301NW8NNT11%O4=M
2301

OS:NW8ST11%O5=M2301NW8ST11%O6=M2301ST11)WIN(W1=2000%W2=2000%W3=2
000%W4=2000

OS:%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M2301NW8NNS
%CC=N%Q=)T1(R=Y%D

OS:F=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z
%A=S%F=AR%O=%RD=0

OS:%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y
%DF=Y%T=80%W=0%S=

OS:A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR
%O=%RD=0%Q=)T6(R=

OS:Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y
%T=80%W=0%S=Z%A=S+%F=A

OS:R%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G
%RIPCK=G%RUCK=G%R

OS:UD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: -2s, deviation: 0s, median: -3s

| ms-sql-info:

| Windows server name: PRD02

| 10.0.0.247\EPOSERVER:

| Instance name: EPOSERVER

| Version:

| name: Microsoft SQL Server 2005 SP3

| number: 9.00.4035.00

| Product: Microsoft SQL Server 2005

| Service pack level: SP3

| Post-SP patches applied: false

| TCP port: 49231

| Named pipe: \\10.0.0.247\pipe\MSSQL$EPOSERVER\sql\query

|_ Clustered: false

|_nbstat: NetBIOS name: PRD02, NetBIOS user: <unknown>, NetBIOS MAC: 0a:83:d4:26:3c:22 (unknown)

| smb-os-discovery:

| OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)

| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1

| Computer name: PRD02

| NetBIOS computer name: PRD02\x00

| Domain name: blustar.com

| Forest name: blustar.com

| FQDN: PRD02.blustar.com

|_ System time: 2019-05-16T23:38:36+00:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2019-05-16 23:38:36

|_ start_date: 2019-05-15 15:12:29

TRACEROUTE

HOP RTT ADDRESS

1 1.04 ms 10.0.0.247

UDP Scan

Nmap scan report for 10.0.0.1

Host is up (0.00033s latency).

All 100 scanned ports on 10.0.0.1 are open|filtered

MAC Address: 0A:74:B6:47:86:4A (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.33 ms 10.0.0.1

Nmap scan report for 10.0.0.2

Host is up (0.00086s latency).

Not shown: 99 open|filtered ports

PORT STATE SERVICE VERSION

53/udp open domain ISC BIND

|_dns-recursion: Recursion appears to be enabled

MAC Address: 0A:74:B6:47:86:4A (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.86 ms 10.0.0.2

Nmap scan report for 10.0.0.10

Host is up (0.00073s latency).

Not shown: 97 open|filtered ports

PORT STATE SERVICE VERSION

53/udp open domain (generic dns response: SERVFAIL)

|_dns-recursion: Recursion appears to be enabled

| fingerprint-strings:

| DNSVersionBindReq:

| version

| bind

| NBTStat:

|_ CKAAAAAAAAAAAAAAAAAAAAAAAAAAAA

88/udp open kerberos-sec Microsoft Windows Kerberos (server time: 2019-05-17 02:39:58Z)

123/udp open ntp NTP v3

| ntp-info:

|_

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-UDP:V=7.70%I=7%D=5/17%Time=5CDE1B2C%P=x86_64-pc-linux-gnu %r(DNSV

SF:ersionBindReq,1E,"\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x04bind\0

SF:\0\x10\0\x03")%r(NBTStat,32,"\x80\xf0\x80\x82\0\x01\0\0\0\0\0\0\x20CKAA

SF:AAAAAAAAAAAAAAAAAAAAAAAAAA\0\0!\0\x01");

MAC Address: 0A:09:5D:E3:76:80 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: 2s, deviation: 0s, median: 2s

TRACEROUTE

HOP RTT ADDRESS

1 0.73 ms 10.0.0.10

Nmap scan report for 10.0.0.11

Host is up (0.0013s latency).

Not shown: 98 closed ports

PORT STATE SERVICE VERSION

68/udp open|filtered dhcpc

5353/udp open|filtered zeroconf

MAC Address: 0A:D5:2C:1A:91:7A (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 1.31 ms 10.0.0.11

Nmap scan report for 10.0.0.21

Host is up (0.00061s latency).

Not shown: 99 closed ports

PORT STATE SERVICE VERSION

68/udp open|filtered dhcpc

MAC Address: 0A:FD:F0:80:ED:00 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.61 ms 10.0.0.21

Nmap scan report for 10.0.0.23

Host is up (0.00039s latency).

All 100 scanned ports on 10.0.0.23 are open|filtered

MAC Address: 0A:49:B1:79:62:C0 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.39 ms 10.0.0.23

Nmap scan report for 10.0.0.26

Host is up (0.00046s latency).

Not shown: 99 closed ports

PORT STATE SERVICE VERSION

68/udp open|filtered dhcpc

MAC Address: 0A:45:4D:E3:73:E6 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.46 ms 10.0.0.26

Nmap scan report for 10.0.0.186

Host is up (0.00082s latency).

Not shown: 99 closed ports

PORT STATE SERVICE VERSION

68/udp open|filtered dhcpc

MAC Address: 0A:29:7A:A8:BB:32 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.82 ms 10.0.0.186

Nmap scan report for 10.0.0.216

Host is up (0.00044s latency).

Not shown: 99 closed ports

PORT STATE SERVICE VERSION

68/udp open|filtered dhcpc

MAC Address: 0A:71:65:F9:C1:F0 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.44 ms 10.0.0.216

Nmap scan report for 10.0.0.229

Host is up (0.00062s latency).

All 100 scanned ports on 10.0.0.229 are open|filtered

MAC Address: 0A:1C:74:2B:18:44 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Host script results:

|_nbstat: NetBIOS name: DEV01, NetBIOS user: <unknown>, NetBIOS MAC: 0a:1c:74:2b:18:44 (unknown)

TRACEROUTE

HOP RTT ADDRESS

1 0.62 ms 10.0.0.229

Nmap scan report for 10.0.0.247

Host is up (0.00063s latency).

Not shown: 94 closed ports

PORT STATE SERVICE VERSION

123/udp open|filtered ntp

137/udp open|filtered netbios-ns

138/udp open|filtered netbios-dgm

500/udp open|filtered isakmp

1434/udp open ms-sql-m Microsoft SQL Server 9.00.4035.00 (ServerName: PRD02; TCPPort: 49231)

4500/udp open|filtered nat-t-ike

MAC Address: 0A:83:D4:26:3C:22 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| ms-sql-info:

| Windows server name: PRD02

| 10.0.0.247\EPOSERVER:

| Instance name: EPOSERVER

| Version:

| name: Microsoft SQL Server 2005 SP3

| number: 9.00.4035.00

| Product: Microsoft SQL Server 2005

| Service pack level: SP3

| Post-SP patches applied: false

| TCP port: 49231

| Named pipe: \\10.0.0.247\pipe\MSSQL$EPOSERVER\sql\query

|_ Clustered: false

|_nbstat: NetBIOS name: PRD02, NetBIOS user: <unknown>, NetBIOS MAC: 0a:83:d4:26:3c:22 (unknown)

TRACEROUTE

HOP RTT ADDRESS

1 0.63 ms 10.0.0.247

Nmap scan report for 10.0.0.72

Host is up (0.000033s latency).

Not shown: 98 closed ports

PORT STATE SERVICE VERSION

68/udp open|filtered dhcpc

5353/udp open|filtered zeroconf

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done at Fri May 17 03:09:12 2019 -- 256 IP addresses (12 hosts up) scanned in 2840.89 seconds