Nama : Leny Novita Sari
NIM : 09011181320027
Keamanan Jaringan Komputer

Network Scanning and CVE

(Common Vulnerabilities and Exposures List)

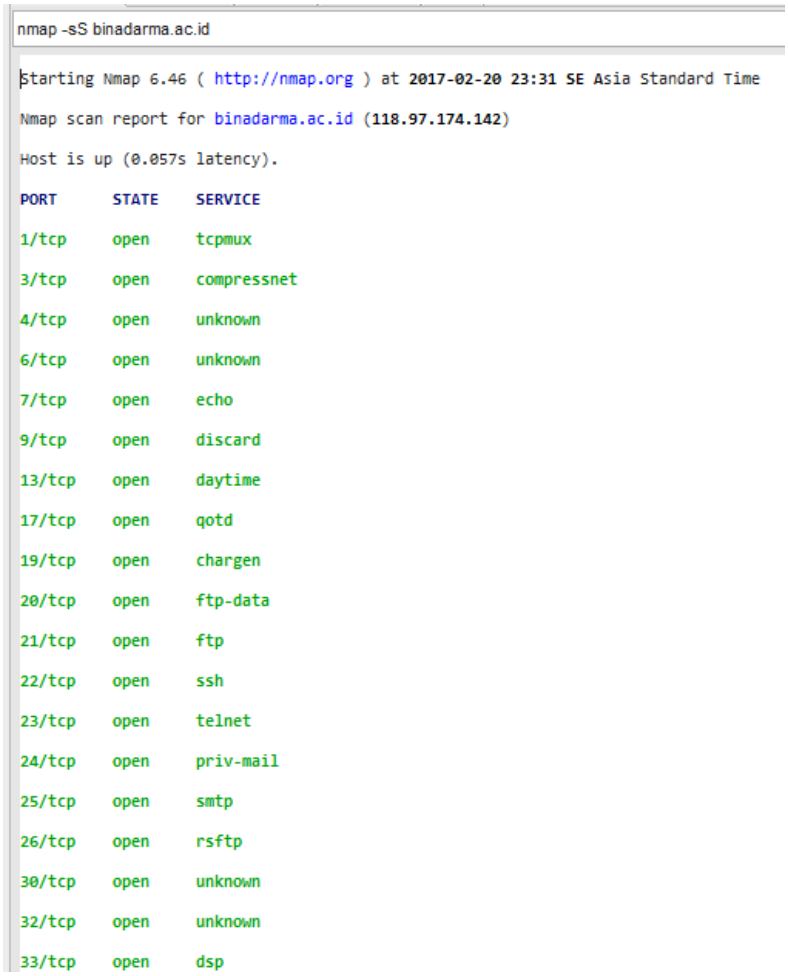
Scanning dan memeriksa jaringan target untuk mengekspos beberapa celah keamanan pada mesin target. Tindakan yang berupa penyelidikan informasi termasuk pengujian sistem untuk beberapa jenis respon, *port sanning, active daemon* dan menguji sitem dengan mengirimkan berbagai query pada target. *Acknowledgement flow* dapat bekerja dengan mengamati kegagalan pesan yang datang kembali ke sistem ketika masalah pengiriman telah terdeteksi. Tujuan dari tahap ini adalah untuk menemukan dimana target yang paling rentan, informasi tersebut kemudian dapat digunakan dalam hubungannya dengan CERT *Vulnerability Notes Database,* CVE *(Common Vulnerabilities and Exposures List), metasploit* dan *the security community (CVE, Security Focus, National Vulnerability Database, Secunia, Microsoft Security Bulletin and Exploit search)* untuk mencari tahu cara terbaik untuk mendapatkan akses pada mesin target.

Target : binadarma.ac.id (target tetap sama seperti step sebelumnya)

Scanning yang dilakukan menggunakan OS windows yang dibantu oleh *tools* zenmap dimana *tools* ini akan digunakan untuk *scanning open port* dan daemon. Dari proses *scanning* yang dilakukan, 1000 *open port* yang didapatkan dari proses *scanning* pada binadarma.ac.id mayoritas menggunakan protokol TCP.

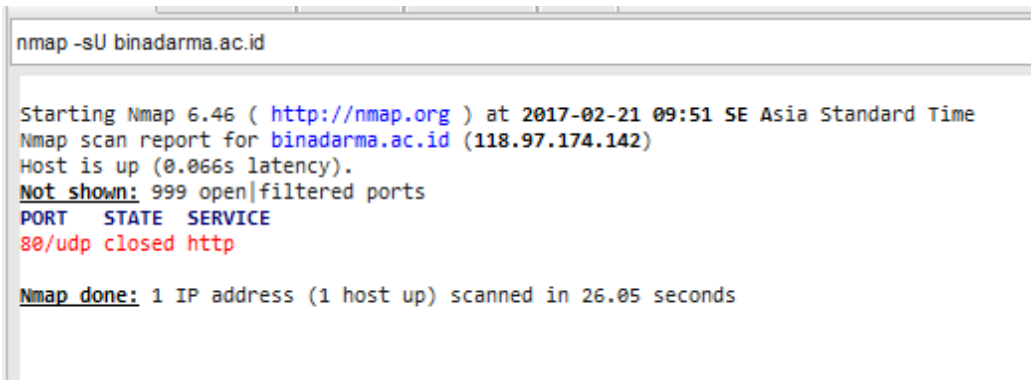
Gambar.1 Scanning binadarma.ac.id

Dengan menggunakan perintah –sS pada zenmap, TCP SYN akan digunakan untuk mendeteksi port apa saja yang terbuka tanpa membuka hubungan komunikasi TCP/IP secara penuh, seperti gambar.2. Teknik ini hampir tidak terdeteksi oleh host target yang tidak mencatat aktivitas portnya secara maksimal atau dengan kata lain ini merupakan scan yang tidak terdeteksi.



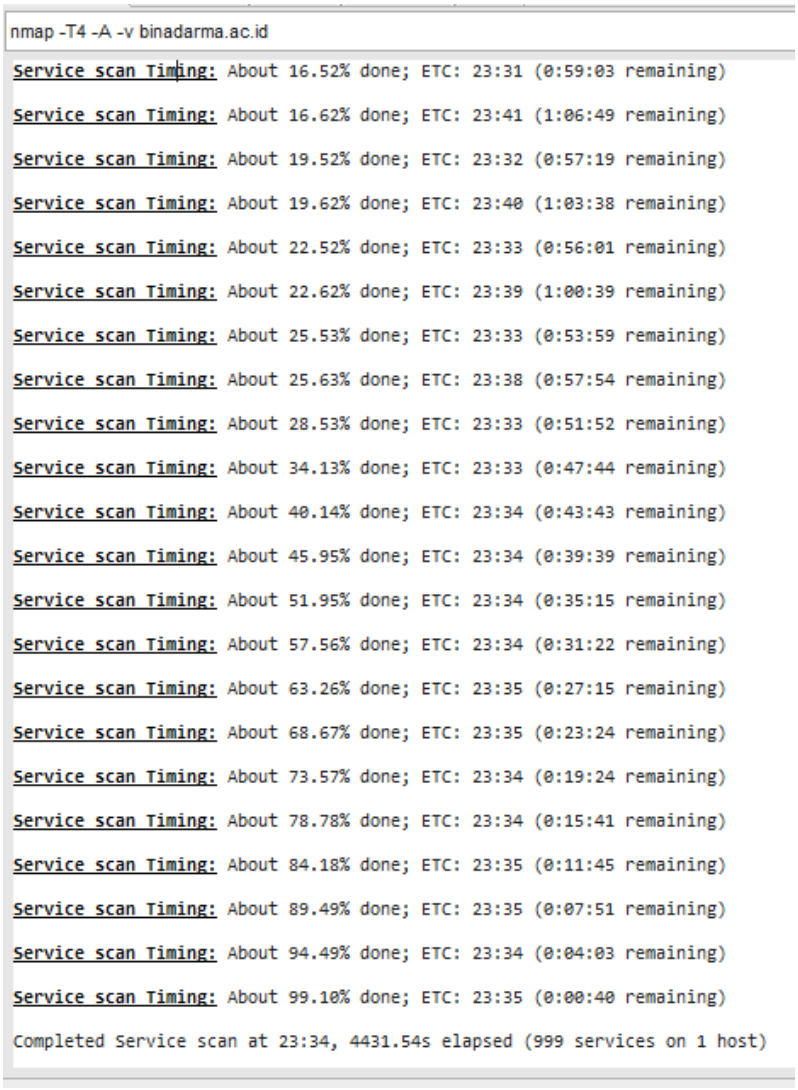
Gambar.2 Openport pada binadarma.ac.id

Hasil proses *scanning* mayoritas menggunakan protokol TCP, tetapi kita bisa melakukan UDP scan dengan perintah –sU. Teknik ini mengirimkan suatu paket UDP ke port host target. Hasil scan pada target saya, ada 1 port yaitu port 80 sebagai layanan browsing (http) pada binadarma.ac.id yang menggunakan protokol UDP namun berstatus close.



Gambar.2 UDP Scan

Selain mendeteksi port, zenmap juga dapat mendeteksi servis-servis yang berjalan pada target seperti pada Gambar.3.



Gambar.3 Service Scan

Setelah melakukan *service scanning* seperti gambar.3, terdapat 999 servis pada binadarma.ac.id seperti yang terlihat pada gambar diatas. Servis-servis yang berjalan berupa : 3d-nfsd, 3exmp, abarsd, abyss, acc-raid, accessbuilder, acmsoda, active-net, activesync, admd, admdog, admeng, adobeserver-1, adobeserver-3, advocentkvm, aeroflight-ads, afp, afrog, afs3-bos, afs3-callback, afs3-fileserver, afs3-prserver, agentx, airtport-admin, ajp 12, ajp 13, alias, amandaidx, amiganetfs, ams, amt-esd-prot, amt-soap-http, amt-soap-https, anet, ansoft-lm-1, ansoft-lm-2, ansyslmd, aol, apc-2160, apc-2260, apc-agent, apcupsd, apex-mesh, apocd, apple-sasl, bgp, realserver, pop2, pop3, mysql, msql-cluster, mysql-cm-agent,

nameserver, nessus, netbackup, multiling-http, mailbox, login, lotusmtap, LSA-or-term, ftp-proxy, ftps dan servis-servis lainnya.

NSE (Nmap Scripting Engine) port 443 (port sampling) yang tereksekusi seperti Gambar.4. NSE ini berisikan skrip sederhana untuk mengotomatisasi berbagai tugas jaringan.

```
443/tcp   open     ssl/http             Apache httpd 2.4.17 ((Win32) OpenSSL/1.0.2d PHP/5.6.14)
|_auth-owners: ERROR: Script execution failed (use -d to debug)
| http-methods: POST OPTIONS GET HEAD TRACE
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
| http-title: Bad request!
|_Requested resource was https://www.binadarma.ac.id/
| ssl-cert: Subject: commonName=*.binadarma.ac.id/organizationName=Universitas Bina Darma/stateOrProvinceName=South Sumatra/countryName=ID
| Issuer: commonName=GlobalSign Organization Validation CA - SHA256 - G2/organizationName=GlobalSign nv-sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2016-08-20T02:37:02+00:00
| Not valid after:  2018-08-10T07:26:19+00:00
| MD5:   177e ca1f d66b 2559 ef4c a90b 612a af5d
|_SHA-1: d2c8 a087 45a2 7678 25dd 2739 52e4 71ce a591 f1c2
|_ssl-date: 2100-10-16T12:04:17+00:00; +83y237d18h52m13s from local time.
```

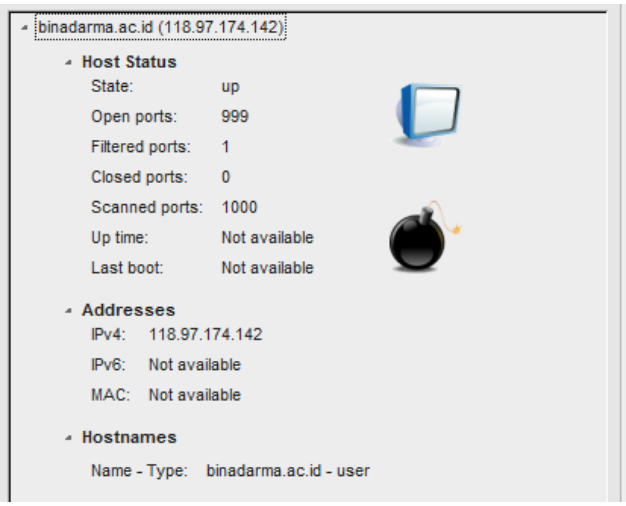
Gambar.4 NSE Port 443

Traceroute yang dilewati paket untuk mencapai tujuan dapat dilihat pada Gambar.5 dibawah ini :

```
TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   6.00 ms   192.168.0.1
2   7.00 ms   192.168.0.1
3   150.00 ms 118.97.174.142
```

Gambar.5 Traceroute port 443

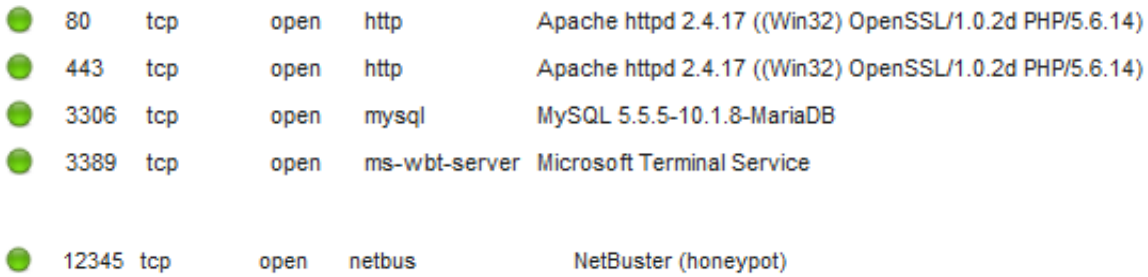
Pada binadarma.ac.id, terdapat 999 *open port* dari 1000 *port* dan 1 *port* yang bersifat *filtered* pada binadarma.ac.id dengan IP 118.97.174.142. 1 *port* yang bersifat *filtered* tersebut adalah port 5555 pada service freeciv.



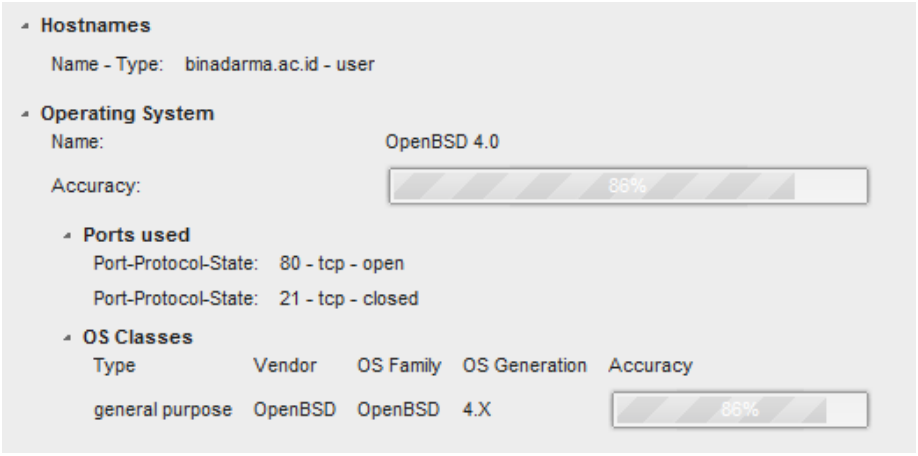
Gambar.6 Detail Host binadarma.ac.id

Gambar.7 Port Filtered

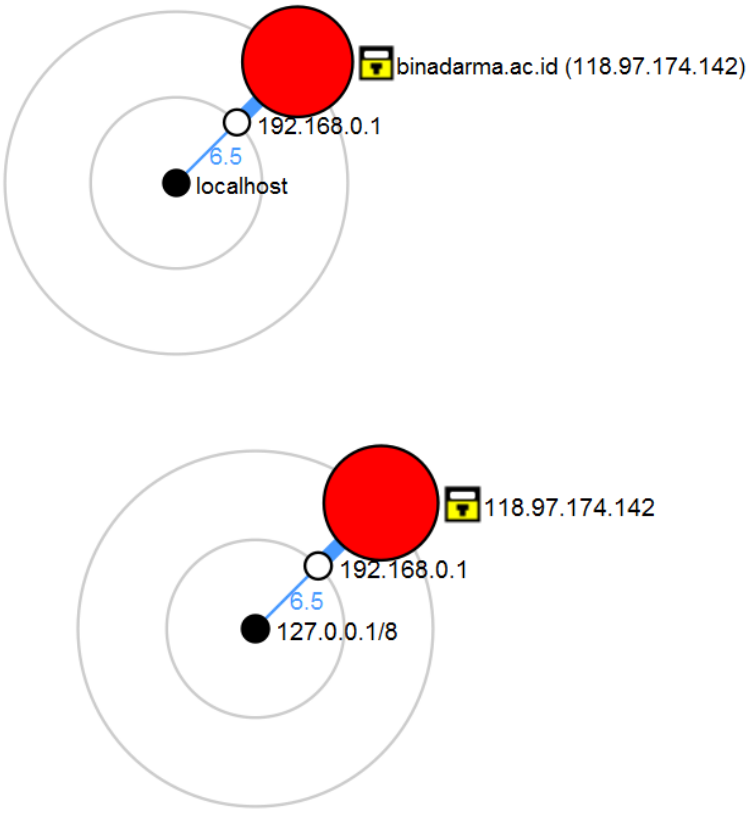
Dari *scanning port* terdapat beberapa daemon dalam sebuah port yang mendukung situs target, yaitu : Apache httpd 2.4.17 ((Win32) OpenSSL/1.0.2d PHP/5.614), MySQL 5.5.5-10.1.8-MarialDB, Microsoft Terminal Service, NetBuster (honey pot) seperti Gambar.8 dengan OpenBSD 4.0 sebagai OS yang digunakan binadarma.ac.id seperti Gambar.9.



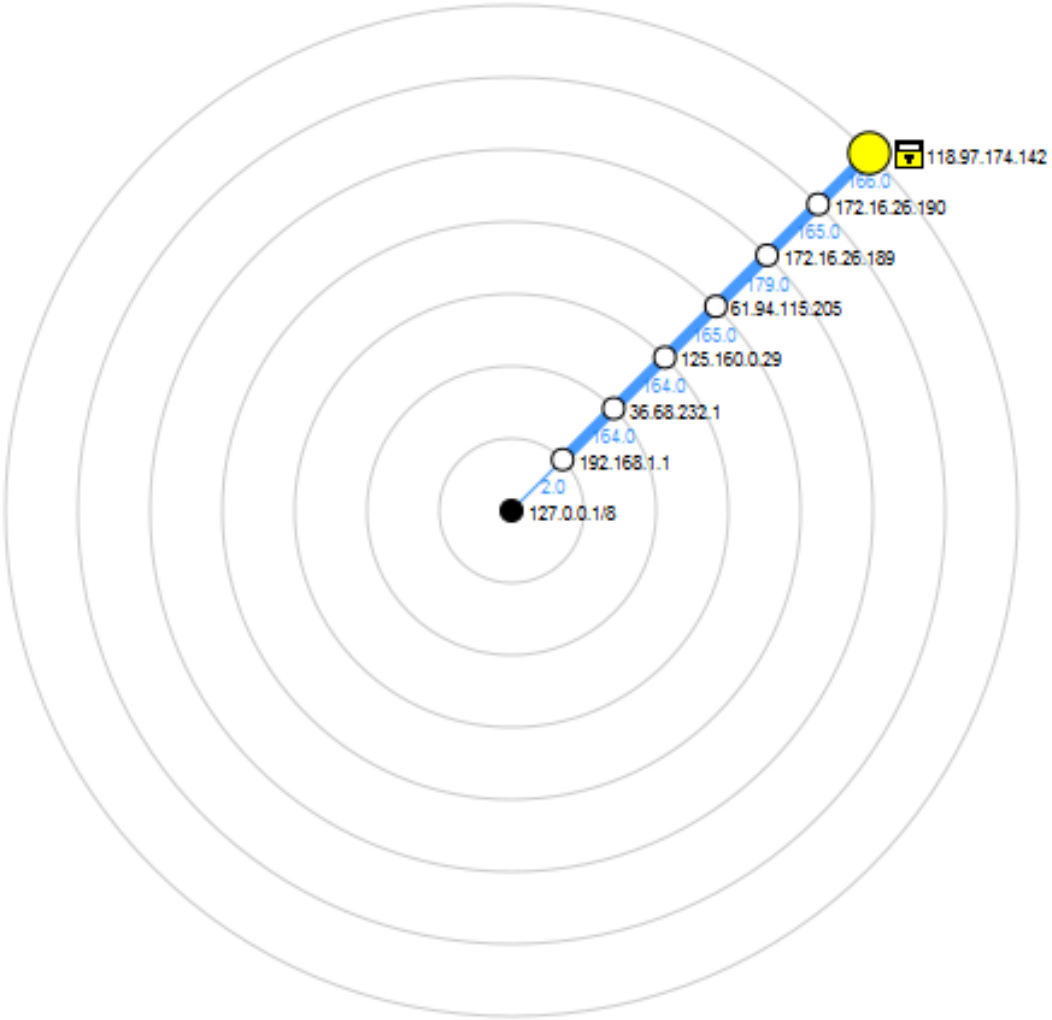
Gambar.8 Daemon binadarma.ac.id



Gambar.9 OS Detection pada binadarma.ac.id



Gambar.10 Gambaran Topologi binadarma.ac.id (1)



Gambar.11 Gambaran Topologi binadarma.ac.id (2)

CVE (Common Vulnerabilities and Exposures List)

Jenis OS	CVE Name	Deskripsi
OpenBSD 4.0	CVE-2007-5365	Fungsi _dl_unsetenv dalam loader.c dalam ld.so ELF pada OpenBSD 3.9 dan 4.0 tidak menghapus lingkungan variabel yang memungkinkan pengguna lokal untuk melewati variabel berbahaya seperti LD_PRELOAD untuk proses loading yang mungkin dimanfaatkan untuk mendapatkan hak.

	CVE-2007-1365	Buffer overflow dalam kern / uipc_mbuf2.c pada OpenBSD 3.9 dan 4.0 memungkinkan penyerangan jarak jauh untuk mengeksekusi kode arbitrary via paket IPv6 karena "salah penanganan mbuf untuk paket ICMP6".
	CVE-2007-5365	Stack berbasis buffer overflow dalam fungsi cons_options di options.c dalam dhcpd pada OpenBSD 4.0 dan 4.2, beberapa implementasi dhcpd lain berdasarkan ISC dhcp-2, memungkinkan penyerang remote untuk mengeksekusi kode arbitrary atau menyebabkan penolakan layanan (daemon crash) melalui permintaan DHCP, menentukan ukuran pesan maksimum lebih kecil dari minimum IP MTU.

Jenis Daemon	**CVE Name**	**Deskripsi**
Apache httpd 2.4.17 ((Win32) OpenSSL/1.0.2d PHP/5.614)	CVE-2016-1546	Apache HTTP Server 2.4.17 dan 2.4.18, ketika mod_http2 diaktifkan, tidak membatasi jumlah stream worker secara simultan untuk HTTP / 2 koneksi tunggal, yang memungkinkan penyerang remote untuk penolakan layanan (stream pengolahan outage) melalui modifikasi window flow-control.
	CVE-2016-8740	Modul mod_http2 di Apache HTTP Server 2.4.17 melalui 2.4.23, ketika konfigurasi Protokol termasuk h2 atau H2C, tidak membatasi panjang permintaan-header, yang memungkinkan penyerang remote untuk penolakan layanan (konsumsi memori) melalui CONTINUATION yang dibuat frame dalam HTTP / 2 permintaan.
MySQL 5.5.5-10.1.8-MarialDB	CVE-2016-6662	Oracle MySQL melalui 5.5.52, 5.6.x melalui 5.6.33, dan 5.7.x melalui 5.7.15; MariaDB sebelum 5.5.51, 10.0.x sebelum 10.0.27, dan 10.1.x sebelum 10.1.17; dan Percona Server sebelum 5.5.51-38.1, 5.6.x sebelum 5.6.32-78.0, dan 5.7.x sebelum 5.7.14-7

		memungkinkan pengguna lokal untuk membuat konfigurasi sewenang-wenang dan mengabaikan mekanisme perlindungan tertentu dengan menetapkan general_log_file untuk my.cnf sebuah konfigurasi. CATATAN: ini dapat dimanfaatkan untuk mengeksekusi kode arbitrary dengan hak akses root dengan menetapkan malloc_lib.
	CVE-2016-6663	Kondisi balapan di Oracle MySQL sebelum 5.5.52, 5.6.x sebelum 5.6.33, 5.7.x sebelum 5.7.15, dan 8.x sebelum 8.0.1; MariaDB sebelum 5.5.52, 10.0.x sebelum 10.0.28, dan 10.1.x sebelum 10.1.18; Percona Server sebelum 5.5.51-38.2, 5.6.x sebelum 5.6.32-78-1, dan 5.7.x sebelum 5.7.14-8; dan Percona XtraDB Cluster sebelum 5.5.41-37.0, 5.6.x sebelum 5.6.32-25.17, dan 5.7.x sebelum 5.7.14-26.17 memungkinkan pengguna lokal dengan izin tertentu untuk mendapatkan hak dengan memanfaatkan penggunaan my_copystat oleh REPAIR TABLE untuk memperbaiki tabel MyISAM.