TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA : AGUS JULIANSYAH

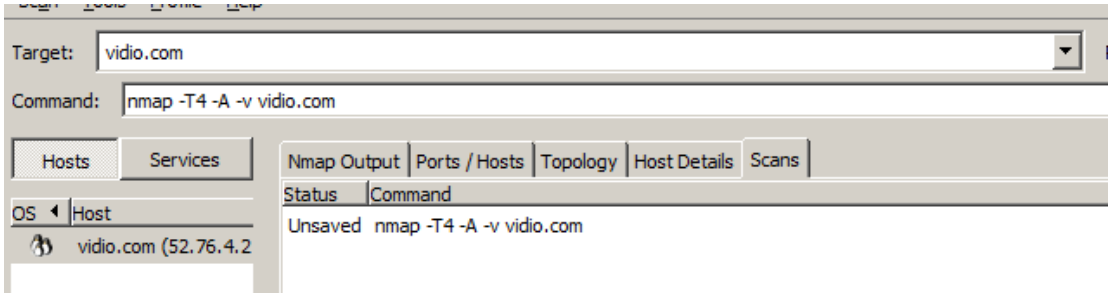
NIM : 09011181320034

KELAS : SK8A

JURUSAN SISTEM KOMPUTER
FAKUTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

Lakukan scanning pada user/ target

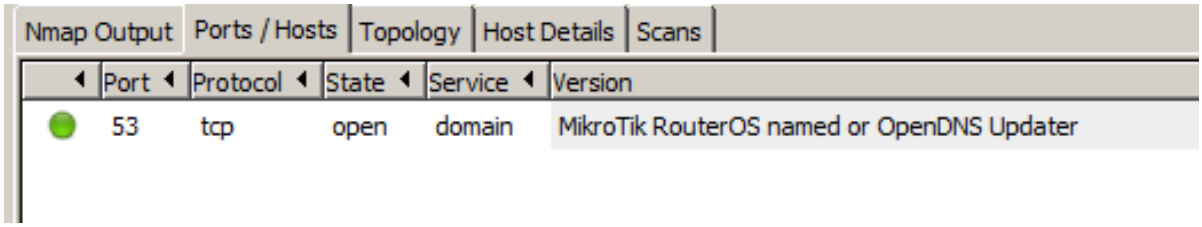
Jawaban



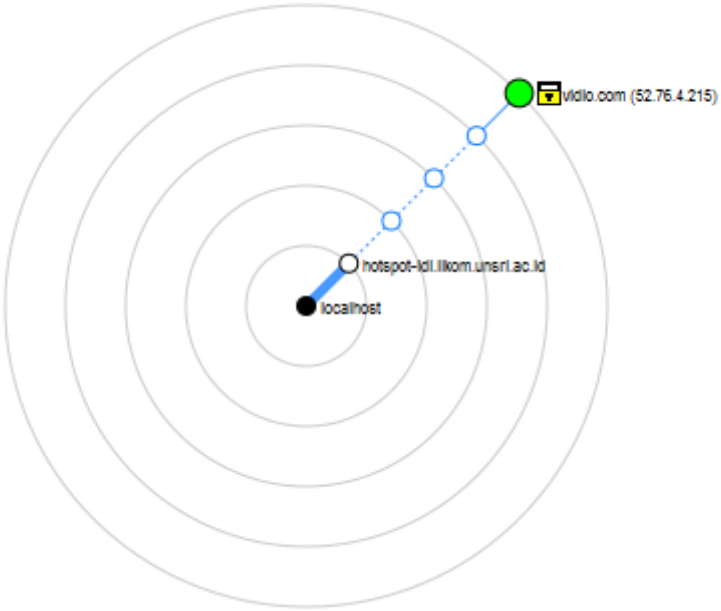
Dari hasil scanning diatas dengan menggunakan domain vidio.com di lakukan dengan scan menggunakan nmap dapat menhasilkan scanan nya yaitu Unsaved nmap -T4 -A -v vidio.comdan IP nya vidio.com (52.76.4.215).

```
nmap -T4 -A -v vidio.com

Starting Nmap 6.46 ( http://nmap.org ) at 2017-02-22 17:08 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 17:08
Scanning vidio.com (52.76.4.215) [4 ports]
Completed Ping Scan at 17:08, 1.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:09
Completed Parallel DNS resolution of 1 host. at 17:09, 1.66s elapsed
Initiating SYN Stealth Scan at 17:09
Scanning vidio.com (52.76.4.215) [1000 ports]
Discovered open port 53/tcp on 52.76.4.215
Completed SYN Stealth Scan at 17:09, 4.46s elapsed (1000 total ports)
Initiating Service scan at 17:09
Scanning 1 service on vidio.com (52.76.4.215)
Completed Service scan at 17:09, 6.11s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against vidio.com (52.76.4.215)
Retrying OS detection (try #2) against vidio.com (52.76.4.215)
Initiating Traceroute at 17:09
Completed Traceroute at 17:09, 3.01s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 17:09
Completed Parallel DNS resolution of 2 hosts. at 17:09, 0.02s elapsed
NSE: Script scanning 52.76.4.215.
Initiating NSE at 17:09
Completed NSE at 17:09, 16.13s elapsed
Nmap scan report for vidio.com (52.76.4.215)
Host is up (0.033s latency).
rDNS record for 52.76.4.215: ec2-52-76-4-215.ap-southeast-1.compute.amazonaws.com
Not shown: 999 filtered ports
PORT    STATE SERVICE VERSION
53/tcp open  domain  MikroTik RouterOS named or OpenDNS Updater
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.31 - 2.6.35 (99%), Linux 2.6.32 (99%), HP P2000 G3 NAS device (96%), Linux 2.6.19 - 2.6.36 (94%), Citrix XenServer (Linux 2.6.18) (93%), Linux 2.6.15 - 2.6.30
(93%), Linux 2.6.22 - 2.6.36 (93%), Linux 2.6.23 - 2.6.38 (93%), Linux 2.6.32 - 2.6.33 (92%), Check Point VPN-1 UTM appliance (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 60.964 days (since Fri Dec 23 18:01:13 2016)
Network Distance: 5 hops
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   37.00 ms hotspot-id1.ilkom.unsri.ac.id (10.100.224.1)
2   ... 4
5   30.00 ms ec2-52-76-4-215.ap-southeast-1.compute.amazonaws.com (52.76.4.215)

NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.84 seconds
           Raw packets sent: 2088 (95.460KB) | Rcvd: 42 (2.686KB)
```

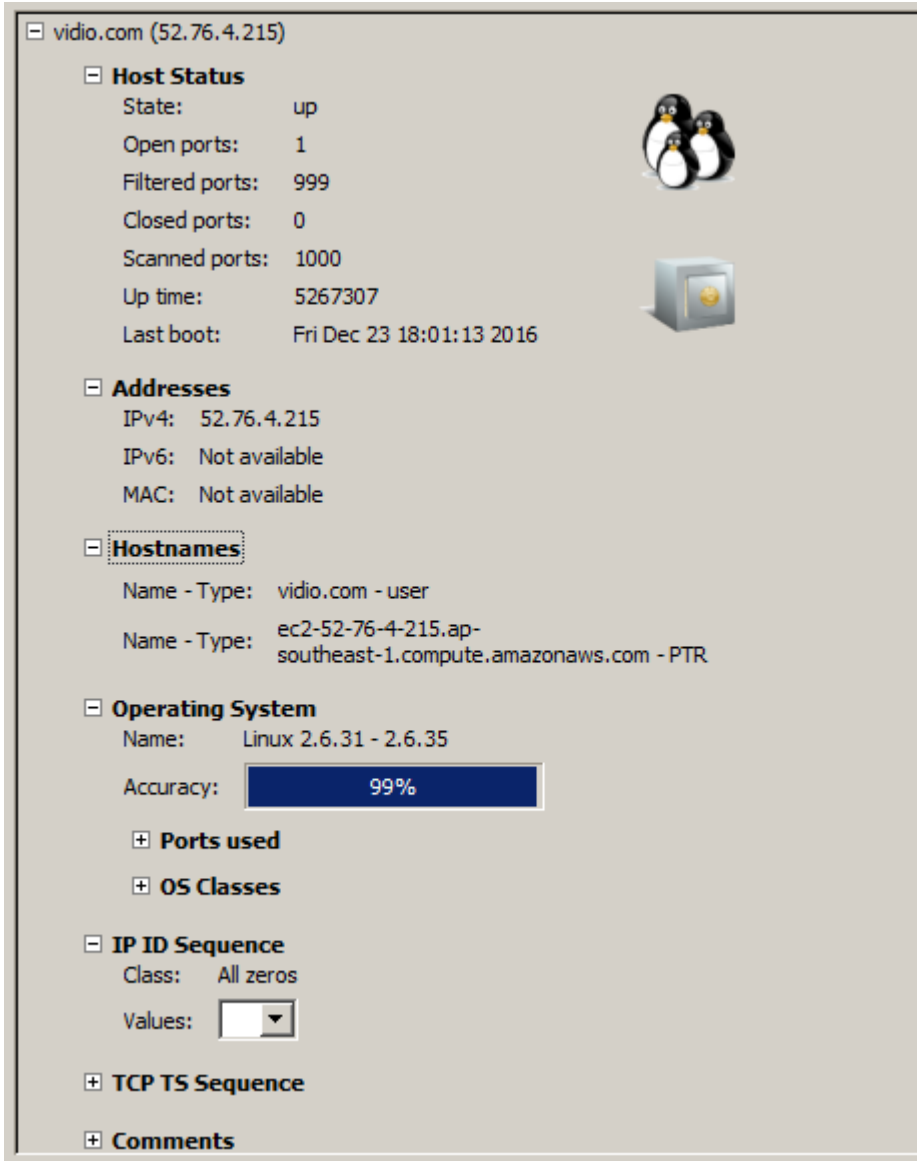
Jawaban: hasil gambar di atas scanan di atas bahwa dengan menggunakan domain vidio.com di lakukan dengan local host (http://nmap.org}, scanning vidio.com juga memiliki IP (52.76.4.215) (4port) dan ada juga (1000 port), data diatas juga memiliki traceroute (using port 53/tcp): HOP ritnya 37.00 ms yg menggunakan IP address hotspot-idl-ilkom-unsri.ac.id dan 30.00 ms ec2-52-76-4-215.ap-southeast-1.compute.amazonaws.com (52.76.4.215),



Jawaban: hasil scanning menggunakan domain vidio.com menghasilkan portnya 53, protocol nya tcp, state nya open , servicenya domain dan versionnya mikrotik routerOS named or open DNS updater dari domain vidio.com tersbut.



Jawaban: dari hasil scanning di atas dapat saya lihat bahwa user localhost berkomunikasi dengan domain vidio.com dan IP nya (52.76.4.215) menggunkan jaringan local hotspot-idl-fasilkom-unsri.ac.id untuk saling berkomunikasi.



Jawaban: Dari hasil gambar di atas yang menggukan domain vidio.com saya dapat melihat host statusnya yaitu ada state up, ipen port, filtered port(999), closed port, scannet portnya (1000) dan memiliki IP Address nya (IPv4 52.76.4.215) , IPv6 nya no available dan MAC nya no available. Memiliki hostnames : name-type : vidio.com-user, ec2-52-76-4-215 dan operasi systremnya linux 2.6.31-2.6.35.

Tampilan CVE.

Search Results

There are **1** CVE entries that match your search.

Name	Description
CVE-2013-6795	The Updater in Rackspace Openstack Windows Guest Agent for XenServer before 1.2.6.0 allows remote attackers to execute arbitrary code via a crafted serialized .NET object to TCP port 1984, which triggers the download and extraction of a ZIP file that overwrites the Agent service binary.

Search Results

There are **11** CVE entries that match your search.

Name	Description
CVE-2016-4350	Multiple SQL injection vulnerabilities in the Web Services web server in SolarWinds Storage Resource Monitor (SRM) Profiler (formerly Storage Manager (STM)) before 6.2.3 allow remote attackers to execute arbitrary SQL commands via the (1) ScriptSchedule parameter in the ScriptServlet servlet; the (2) winEventId or (3) winEventLog parameter in the WindowsEventLogsServlet servlet; the (4) processOS parameter in the ProcessesServlet servlet; the (5) group, (6) groupName, or (7) clientName parameter in the BackupExceptionsServlet servlet; the (8) valDB or (9) valFS parameter in the BackupAssociationServlet servlet; the (10) orderBy or (11) orderDir parameter in the HostStorageServlet servlet; the (12) fileName, (13) sortField, or (14) sortDirection parameter in the DuplicateFilesServlet servlet; the (15) orderFld or (16) orderDir parameter in the QuantumMonitorServlet servlet; the (17) exitCode parameter in the NbuErrorMessageServlet servlet; the (18) udfName, (19) displayName, (20) udfDescription, (21) udfDataValue, (22) udfSectionName, or (23) udfId parameter in the UserDefinedFieldConfigServlet servlet; the (24) sortField or (25) sortDirection parameter in the XiotechMonitorServlet servlet; the (26) sortField or (27) sortDirection parameter in the BexDriveUsageSummaryServlet servlet; the (28) state parameter in the ScriptServlet servlet; the (29) assignedNames parameter in the FileActionAssignmentServlet servlet; the (30) winEventSource parameter in the WindowsEventLogsServlet servlet; or the (31) name, (32) ipOne, (33) ipTwo, or (34) ipThree parameter in the XiotechMonitorServlet servlet.
CVE-2016-3872	Buffer overflow in codecs/on2/dec/SoftVPX.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows attackers to gain privileges via a crafted application, aka internal bug 29421675.
CVE-2016-2452	codecs/amrnb/dec/SoftAMR.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bugs 27662364 and 27843673.
CVE-2016-2451	codecs/on2/dec/SoftVPX.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-05-01 does not validate VPX output buffer sizes, which allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27597103.
CVE-2016-1624	Integer underflow in the ProcessCommandsInternal function in dec/decode.c in Brotli, as used in Google Chrome before 48.0.2564.109, allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted data with brotli compression.
CVE-2016-1238	(1) cpan/Archive-Tar/bin/ptar, (2) cpan/Archive-Tar/bin/ptardiff, (3) cpan/Archive-Tar/bin/ptargrep, (4) cpan/CPAN/scripts /cpan, (5) cpan/Digest-SHA/shasum, (6) cpan/Encode/bin/enc2xs, (7) cpan/Encode/bin/encguess, (8) cpan/Encode /bin/piconv, (9) cpan/Encode/bin/ucmlint, (10) cpan/Encode/bin/unidump, (11) cpan/ExtUtils-MakeMaker/bin/instmodsh, (12) cpan/IO-Compress/bin/zipdetails, (13) cpan/JSON-PP/bin/json_pp, (14) cpan/Test-Harness/bin/prove, (15) dist/ExtUtils-ParseXS/lib/ExtUtils/xsubpp, (16) dist/Module-CoreList/corelist, (17) ext/Pod-Html/bin/pod2html, (18) utils/c2ph.PL, (19) utils/h2ph.PL, (20) utils/h2xs.PL, (21) utils/libnetcfg.PL, (22) utils/perlbug.PL, (23) utils/perldoc.PL, (24) utils/perlivp.PL, and (25) utils/splain.PL in Perl 5.x before 5.22.3-RC2 and 5.24 before 5.24.1-RC2 do not properly remove . (period) characters from the end of the includes directory array, which might allow local users to gain privileges via a Trojan horse module under the current working directory.
CVE-2016-0914	EMC Documentum WebTop 6.8 before Patch 13 and 6.8.1 before Patch 02, Documentum Administrator 7.x before 7.2 Patch 13, Documentum Capital Projects 1.9 before Patch 23 and 1.10 before Patch 10, and Documentum TaskSpace 6.7 SP3 allow remote authenticated users to bypass intended access restrictions and execute arbitrary IAPI/IDQL commands via the IAPI/IDQL interface.
CVE-2016-0882	EMC Documentum xCP 2.1 before patch 23 and 2.2 before patch 11 allows remote authenticated users to read arbitrary files via a POST request containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.
CVE-2016-0881	EMC Documentum xCP 2.1 before patch 23 and 2.2 before patch 11 allows remote authenticated users to conduct Documentum Query Language (DQL) injection attacks and obtain sensitive repository information by appending a query to a REST request.
CVE-2016-0023	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2006-2635	Multiple cross-site scripting (XSS) vulnerabilities in Tikiwiki (aka Tiki CMS/Groupware) 1.9.x allow remote attackers to inject arbitrary web script or HTML via malformed nested HTML tags such as "<scr<script>ipt>" in (1) offset and (2) days parameters in (a) tiki-lastchanges.php, the (3) find and (4) offset parameters in (b) tiki-orphan_pages.php, the (5) offset and (6) initial parameters in (c) tiki-listpages.php, and (7) an unspecified field in (d) tiki-remind_password.php; and allow remote authenticated users with admin privileges to inject arbitrary web script or HTML via (8) an unspecified field in a metatags action in (e) tiki-admin.php, the (9) offset parameter in (f) tiki-admin_rssmodules.php, the (10) offset and (11) max parameters in (g) tiki-syslog.php, the (12) numrows parameter in (h) tiki-adminusers.php, (13) an unspecified field in (i) tiki-adminusers.php, (14) an unspecified field in (j) tiki-admin_hotwords.php, unspecified fields in (15) "Assign new module" and (16) "Create new user module" in (k) tiki-admin_modules.php, (17) an unspecified field in "Add notification" in (l) tiki-admin_notifications.php, (18) the offset parameter in (m) tiki-admin_notifications.php, the (19) Name and (20) Dsn fields in (o) tiki-admin_dsn.php, the (21) offset parameter in (p) tiki-admin_content_templates.php, (22) an unspecified field in "Create new template" in (q) tiki-admin_content_templates.php, and the (23) offset parameter in (r) tiki-admin_chat.php.

Jawban : Dari gambari hasil tampilan CVE diatas memiliki tampilan dan diskripsi yang berbeda-beda.