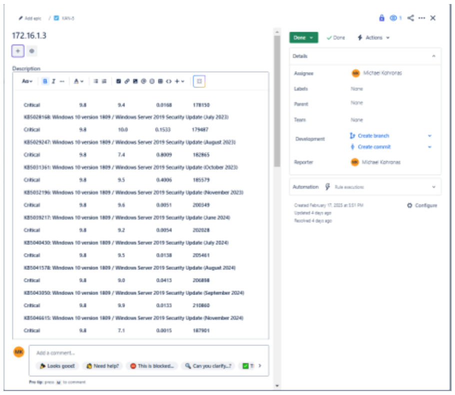
Patched Vulnerabilities – See Mitigations document for in depth step by step

172.16.1.3 – 30m

Updated Windows



Add epic / KAN-5

172.16.1.3

Description

Critical	9.8	9.4	0.0168	178150
KB5028168: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2023)				
Critical	9.8	10.0	0.1533	179487
KB5029247: Windows 10 version 1809 / Windows Server 2019 Security Update (August 2023)				
Critical	9.8	7.4	0.8009	182865
KB5031361: Windows 10 version 1809 / Windows Server 2019 Security Update (October 2023)				
Critical	9.8	9.5	0.4006	185579
KB5032196: Windows 10 version 1809 / Windows Server 2019 Security Update (November 2023)				
Critical	9.8	9.6	0.0051	200349
KB5039217: Windows 10 version 1809 / Windows Server 2019 Security Update (June 2024)				
Critical	9.8	9.2	0.0054	202028
KB5040430: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2024)				
Critical	9.8	9.5	0.0138	205461
KB5041578: Windows 10 version 1809 / Windows Server 2019 Security Update (August 2024)				
Critical	9.8	9.0	0.0413	206898
KB5043050: Windows 10 version 1809 / Windows Server 2019 Security Update (September 2024)				
Critical	9.8	9.9	0.0133	210860
KB5046615: Windows 10 version 1809 / Windows Server 2019 Security Update (November 2024)				
Critical	9.8	7.1	0.0015	187901

Add a comment...

Pro tip: press M to comment

Assignee	Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	Michael Kohronas

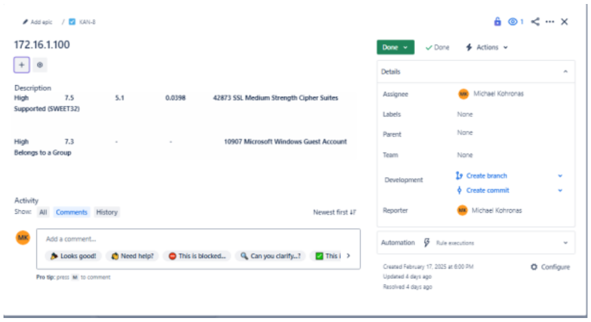
Automation Rule executions

Created February 17, 2025 at 5:51 PM
Updated 4 days ago
Resolved 4 days ago

172.16.1.100 – 20m

Disabled the Vulnerable Cipher through SCHANNEL

Remove groups from guest in lusrmgr.msc



Add epic / KAN-8

172.16.1.100

Description

High	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
High	7.3	-	-	10907	Microsoft Windows Guest Account Belongs to a Group

Activity

Show: All Comments History Newest first

Add a comment...

Pro tip: press M to comment

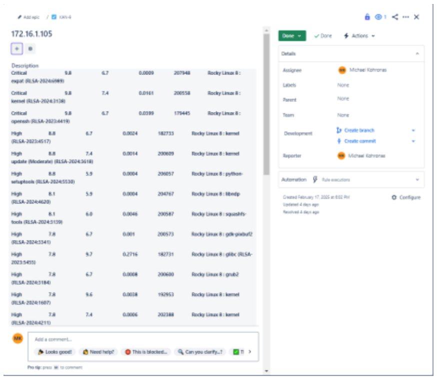
Assignee	Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	Michael Kohronas

Automation Rule executions

Created February 17, 2025 at 6:00 PM
Updated 4 days ago
Resolved 4 days ago

172.16.1.105 – 15m

Sudo yum update



Add epic / KAN-6

172.16.1.105

Description

Critical	9.8	6.7	0.0009	207948	Rocky Linux 8 : expat (RLSA-2024:6989)
Critical	9.8	7.4	0.0161	200558	Rocky Linux 8 : kernel (RLSA-2024:3138)
Critical	9.8	6.7	0.0399	179445	Rocky Linux 8 : openssh (RLSA-2023:4419)
High	8.8	6.7	0.0024	182733	Rocky Linux 8 : kernel (RLSA-2023:4517)
High	8.8	7.4	0.0014	200609	Rocky Linux 8 : kernel update (Moderate) (RLSA-2024:3618)
High	8.8	5.9	0.0004	206057	Rocky Linux 8 : python-setuptools (RLSA-2024:5530)
High	8.1	5.9	0.0004	204767	Rocky Linux 8 : libndp (RLSA-2024:4620)
High	8.1	6.0	0.0046	200587	Rocky Linux 8 : squashfs-tools (RLSA-2024:3139)
High	7.8	6.7	0.001	200573	Rocky Linux 8 : gdk-pixbuf2 (RLSA-2024:3341)
High	7.8	9.7	0.2716	182731	Rocky Linux 8 : glibc (RLSA-2023:5455)
High	7.8	6.7	0.0008	200600	Rocky Linux 8 : grub2 (RLSA-2024:3184)
High	7.8	9.6	0.0038	192953	Rocky Linux 8 : kernel (RLSA-2024:1607)
High	7.8	7.4	0.0006	202388	Rocky Linux 8 : kernel (RLSA-2024:4211)

Add a comment...

Pro tip: press M to comment

Assignee	Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	Michael Kohronas

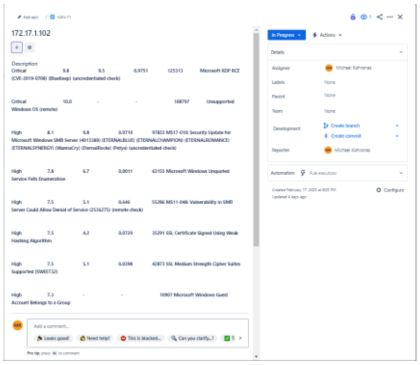
Automation Rule executions

Created February 17, 2025 at 6:02 PM
Updated 4 days ago
Resolved 4 days ago

Unpatched Vulnerabilities

172.17.1.102 – 45m

Needs to be updated to a supported version



172.17.1.102

Description

Critical 9.8 9.5 0.9751 125313 Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Critical 10.0 - - 108797 Unsupported Windows OS (remote)

High 8.1 9.8 0.9719 97833 MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

High 7.8 6.7 0.0011 63155 Microsoft Windows Unquoted Service Path Enumeration

High 7.5 5.1 0.646 55286 MS11-048: Vulnerability in SMB Server Could Allow Denial of Service (2536275) (remote check)

High 7.5 4.2 0.0729 35291 SSL Certificate Signed Using Weak Hashing Algorithm

High 7.5 5.1 0.0398 42873 SSL Medium Strength Cipher Suites Supported (SWEET32)

High 7.3 - - 10907 Microsoft Windows Guest Account Belongs to a Group

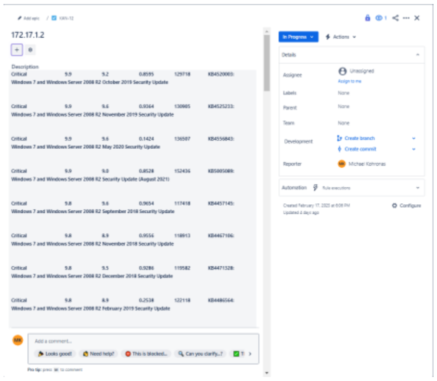
Details

Assignee: Michael Kohronas
Labels: None
Parent: None
Team: None
Development: Create branch, Create commit
Reporter: Michael Kohronas
Automation: Rule executions

Created February 17, 2025 at 6:05 PM
Updated 4 days ago

172.17.1.2 – 0m

Needs to be updated to a supported version



172.17.1.2

Description

Critical 9.9 9.2 0.8595 129718 KB4520003: Windows 7 and Windows Server 2008 R2 October 2019 Security Update

Critical 9.9 9.6 0.9364 130905 KB4525233: Windows 7 and Windows Server 2008 R2 November 2019 Security Update

Critical 9.9 9.6 0.1424 136507 KB4556843: Windows 7 and Windows Server 2008 R2 May 2020 Security Update

Critical 9.9 9.0 0.8528 152436 KB5005088: Windows 7 and Windows Server 2008 R2 Security Update (August 2021)

Critical 9.8 9.6 0.9654 117418 KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update

Critical 9.8 8.9 0.9556 118913 KB4467106: Windows 7 and Windows Server 2008 R2 November 2018 Security Update

Critical 9.8 9.5 0.9286 119582 KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update

Critical 9.8 8.9 0.2538 122118 KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update

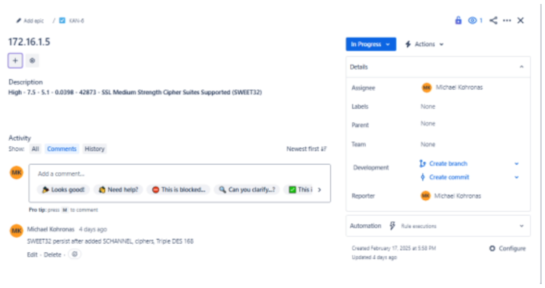
Details

Assignee: Unassigned (Assign to me)
Labels: None
Parent: None
Team: None
Development: Create branch, Create commit
Reporter: Michael Kohronas
Automation: Rule executions

Created February 17, 2025 at 6:08 PM
Updated 4 days ago

172.16.1.5 – 45m

created folders – SCHANNEL, ciphers, Triple DES 168 – creates bar mitzvah vuln



172.16.1.5

Description

High - 7.5 - 5.1 - 0.0398 - 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Activity

Michael Kohronas 4 days ago
SWEET32 persist after added SCHANNEL, ciphers, Triple DES 168

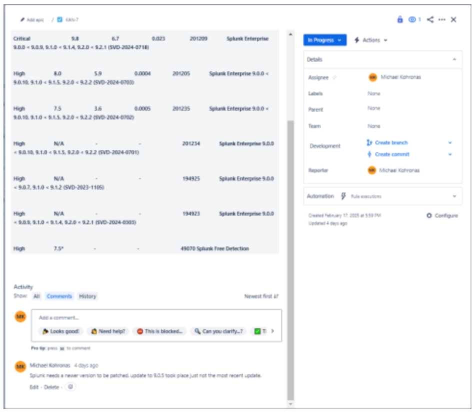
Details

Assignee: Michael Kohronas
Labels: None
Parent: None
Team: None
Development: Create branch, Create commit
Reporter: Michael Kohronas
Automation: Rule executions

Created February 17, 2025 at 5:58 PM
Updated 4 days ago

172.16.1.6 – 1.5h

Stopped splunk services → Installed the new version → Restart Splunk



Critical 9.8 6.7 0.023 201209 Splunk Enterprise 9.0.0 < 9.0.9, 9.1.0 < 9.1.4, 9.2.0 < 9.2.1 (SVD-2024-0718)

High 8.0 5.9 0.0004 201205 Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0703)

High 7.5 3.6 0.0005 201235 Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0702)

High N/A - - 201234 Splunk Enterprise 9.0.0 < 9.0.10, 9.1.0 < 9.1.5, 9.2.0 < 9.2.2 (SVD-2024-0701)

High N/A - - 194925 Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2 (SVD-2023-1105)

High N/A - - 194923 Splunk Enterprise 9.0.0 < 9.0.9, 9.1.0 < 9.1.4, 9.2.0 < 9.2.1 (SVD-2024-0303)

High 7.5* - - 49070 Splunk Free Detection

Activity
Show: All Comments History
Newest first
Add a comment...
Looks good! Need help? This is blocked... Can you clarify...?
Pro tip: press M to comment

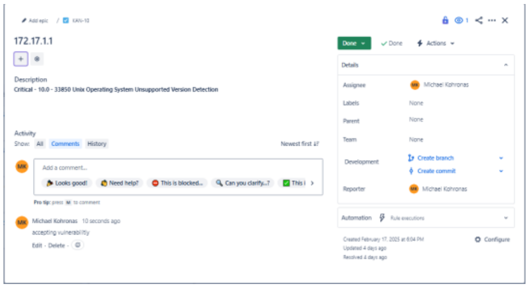
Michael Kohronas 4 days ago
Splunk needs a newer version to be patched. update to 9.0.5 took place just not the most recent update.

Assignee	Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	Michael Kohronas

Created February 17, 2025 at 5:59 PM
Updated 4 days ago

172.17.1.1 / 172.16.1.1 – 0m

Accepting risk as its our firewall and we aren't making changes yet



172.17.1.1

Description
Critical - 10.0 - 33850 Unix Operating System Unsupported Version Detection

Activity
Show: All Comments History
Newest first
Add a comment...
Looks good! Need help? This is blocked... Can you clarify...? This i
Pro tip: press M to comment

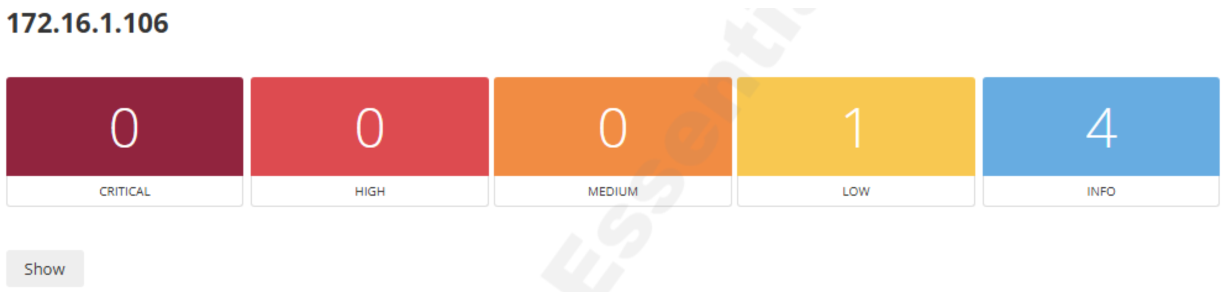
Michael Kohronas 10 seconds ago
accepting vulnerability

Edit · Delete ·
Done
✓ Done
Actions
Details

Assignee	Michael Kohronas
Labels	None
Parent	None
Team	None
Development	Create branch Create commit
Reporter	Michael Kohronas

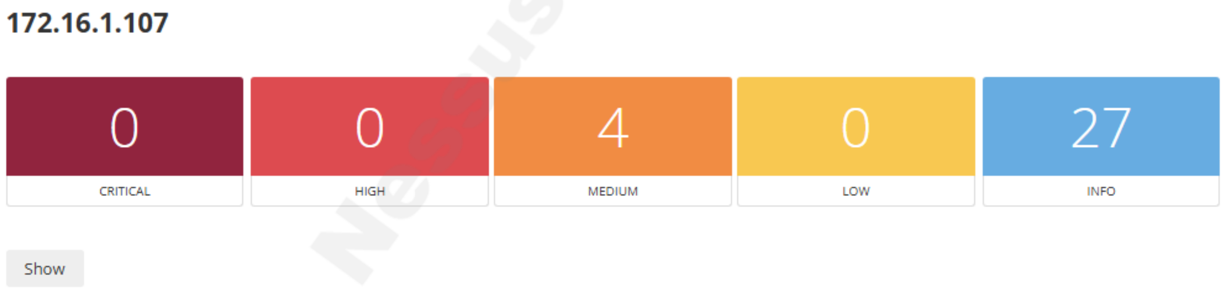
Automation Rule executions
Configure

Created February 17, 2025 at 6:04 PM
Updated 4 days ago
Resolved 4 days ago



172.16.1.106

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	1	4



172.16.1.107

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	27

List the top 5 medium vulnerabilities in the priority order and document why they are in your priority. Next to each item in 4 (above), document what you would do to fix each item.

1. SMB Signing Not Required

- **Why It's Priority:**
  - **Risk Level:** High
  - **Attack Type:** Man-in-the-Middle (MITM), Credential Theft
  - **Affected Hosts:** Multiple hosts, including 172.16.1.100, 172.17.1.102
  - **Impact:** Without SMB signing, attackers can intercept and alter SMB traffic, capturing user credentials or modifying data in transit. This could allow lateral movement and credential theft, leading to domain-wide compromise.
  - **Reason for Priority:** SMB is heavily used in Windows environments. If left unsigned, it enables attackers to impersonate users and escalate privileges, making it a prime target for exploitation in real-world attacks.
- **How to Fix It:**
  - **On Windows Servers:** Set Group Policy "Microsoft network server: Digitally sign communications (always)" to Enabled.
  - **On Windows Clients:** Set Group Policy "Microsoft network client: Digitally sign communications (if server agrees)" to Enabled.
  - **Disable SMBv1:** If still enabled, disable it (Set-SmbServerConfiguration -EnableSMB1Protocol $false).

2. Untrusted SSL Certificate

- **Why It Matters:**
  - **Risk Level:** High
  - **Attack Type:** Remote Exploitation, Brute Force, RDP Hijacking
  - **Affected Hosts:** 172.16.1.100, 172.17.1.102
  - I**mpact:** Without Network Level Authentication (NLA), attackers can attempt RDP connections without credentials, increasing exposure to brute-force attacks and exploits like BlueKeep (CVE-2019-0708). RDP-based ransomware attacks often exploit this misconfiguration.
  - **Reason for Priority:** RDP is a common attack vector. A compromised RDP session can allow attackers full system control, making this a critical misconfiguration that needs immediate remediation.
- **How to Fix It:**
  - **On each RDP server:** Open System Properties > Remote > Require NLA for connections.
  - **Via Group Policy:** Set "Require user authentication for remote connections by using NLA" to Enabled.
  - **Set RDP Encryption to High:** In Group Policy, configure "Encryption level" to High or "SSL/TLS 1.0".
  - **Patch RDP for CVE-2019-0708 (BlueKeep):** Ensure all servers have the latest security updates.
  - **Restrict RDP Access:** Limit RDP to internal networks or VPN users only.
  - **Enable Two-Factor Authentication for RDP:** Consider using MFA solutions to prevent credential theft-based logins.

3. Use of Self-Signed SSL Certificate

- **Why It Matters:**
  - **Risk Level:** Medium-High
  - **Attack Type:** MITM, Downgrade Attacks, Data Decryption
  - **Affected Hosts:** 172.16.1.5, 172.16.1.100, 172.16.1.107, 172.17.1.102
  - **Impact:** TLS 1.0 and 1.1 have known vulnerabilities (e.g., BEAST, POODLE). Attackers can force downgrade connections, decrypt sensitive data, or steal authentication tokens.
  - **Reason for Priority:** Many modern applications no longer support TLS 1.0/1.1, making this a compliance issue (PCI DSS, NIST 800-52r2, HIPAA, etc.) and a security risk.
- **How to Fix It:**
  - **For Windows servers:** Disable TLS 1.0 and 1.1 via registry
    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]
    - "Enabled"=dword:00000000
  - **For Linux servers (Apache/Nginx):** Update SSL config:
    - ssl_protocols TLSv1.2 TLSv1.3;
  - **Ensure Strong Ciphers:** Remove weak ciphers like RC4, DES, 3DES.

4. TLS 1.0 Still Enabled

- **Why It Matters:**
    - **Risk Level:** Medium
    - **Attack Type:** MITM, Downgrade Attack, Session Hijacking
    - **Affected Hosts:** 172.16.1.1, 172.16.1.105
    - **Impact:** Without HTTP Strict Transport Security (HSTS), users can be forced onto HTTP via SSL stripping, allowing attackers to intercept or modify traffic.
    - **Reason for Priority:** HSTS prevents attackers from downgrading connections, forcing HTTPS. Enabling it is an easy fix that significantly improves security.
- **How to Fix It:**
    - **For Apache:** Add to .htaccess or httpd.conf:
        - Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
    - **For Nginx:** Add to nginx.conf:
        - add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;
    - **Ensure All Traffic Uses HTTPS:** Redirect HTTP to HTTPS.

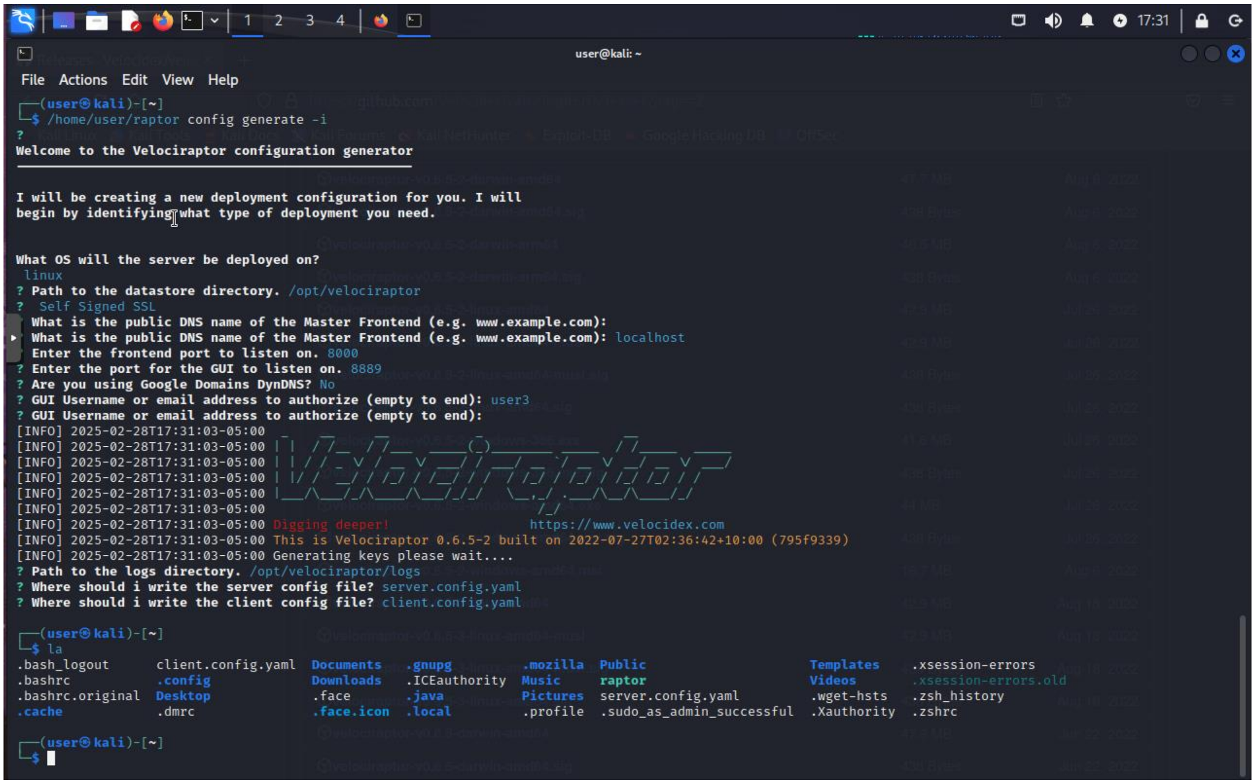
5. NTP Mode 6 Queries Enabled (DDoS Risk)

- **Why It Matters:**
  - **Risk Level:** Medium
  - **Attack Type:** Malware Execution, Code Injection
  - **Affected Hosts:** 172.16.1.3, 172.17.1.2
  - **Impact:** Attackers can append malicious code to signed executables, making them appear legitimate. This bypasses signature verification and allows malware execution.
  - **Reason for Priority:** This vulnerability is actively exploited by malware campaigns to bypass security checks, making it an important fix.
- **How to Fix It:**
  - Apply Microsoft's Security Update for CVE-2013-3900.
  - Set the Registry Key to Force Verification:
    - reg add HKLM\Software\Microsoft\Cryptography\Wintrust\Config /v EnableCertPaddingCheck /t REG_DWORD /d 1 /f

References:

- SMB Signing Not Required
  - https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-security
  - https://nvd.nist.gov/vuln/detail/CVE-2017-0144
- Weak RDP Security (NLA Not Required)
  - https://www.techtarget.com/searchvirtualdesktop/tip/Top-5-remote-desktop-connectivity-problems-and-how-to-prevent-them
  - https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/592a0337-dc91-4de3-a901-e1829665291d
- Outdated TLS Protocols (TLS 1.0/1.1 Enabled)
  - https://csrc.nist.gov/pubs/sp/800/52/r2/final
  - https://learn.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings?tabs=diffie-hellman
- Missing HTTP Strict Transport Security (HSTS) Header
  - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
  - https://hstspreload.org/
- Incomplete WinVerifyTrust Signature Validation
  - https://nvd.nist.gov/vuln/detail/CVE-2013-3900
  - https://learn.microsoft.com/en-us/windows/win32/api/wintrust/nf-wintrust-winverifytrust

Raptor Install



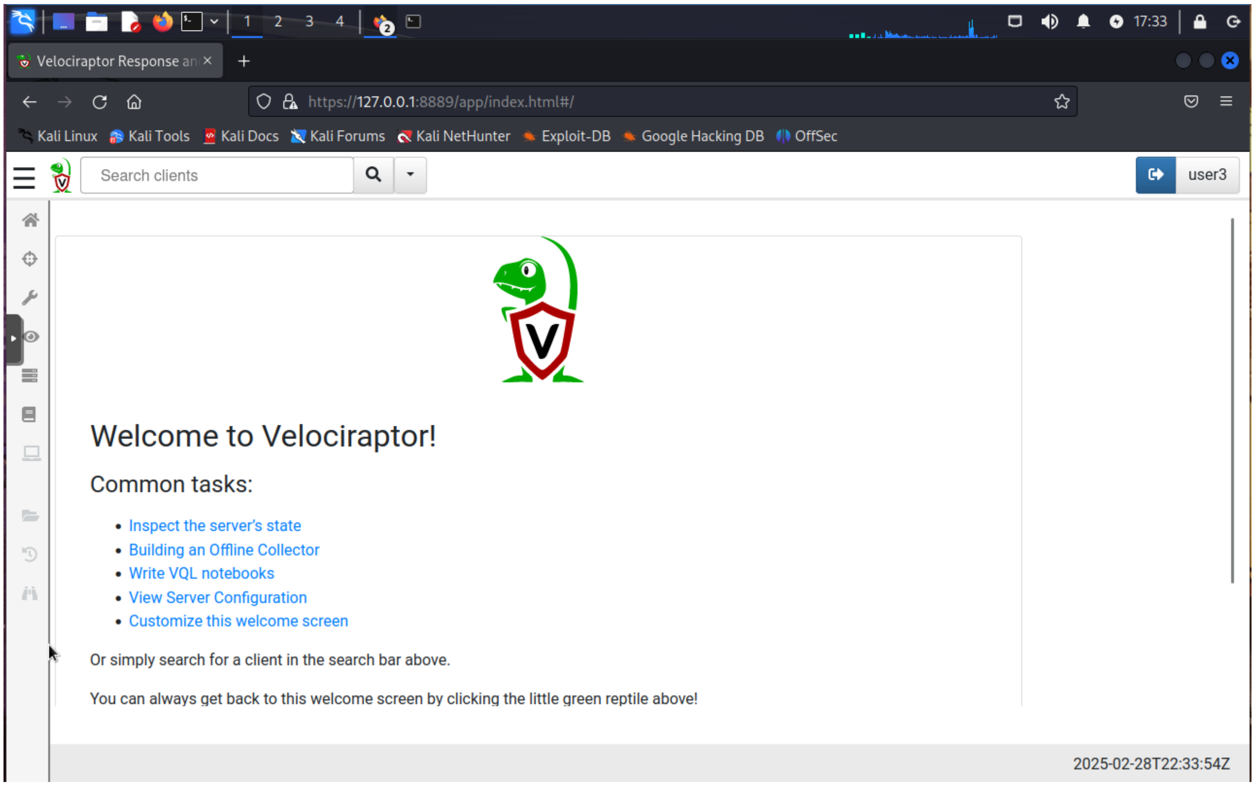
```
┌──(user㉿kali)-[~]
└─$ /home/user/raptor config generate -i
?
Welcome to the Velociraptor configuration generator
───────────────────────────────────────────────────

I will be creating a new deployment configuration for you. I will
begin by identifying what type of deployment you need.


What OS will the server be deployed on?
 linux
? Path to the datastore directory. /opt/velociraptor
?  Self Signed SSL
  What is the public DNS name of the Master Frontend (e.g. www.example.com):
  What is the public DNS name of the Master Frontend (e.g. www.example.com): localhost
  Enter the frontend port to listen on. 8000
? Enter the port for the GUI to listen on. 8889
? Are you using Google Domains DynDNS? No
? GUI Username or email address to authorize (empty to end): user3
? GUI Username or email address to authorize (empty to end):
[INFO] 2025-02-28T17:31:03-05:00
[INFO] 2025-02-28T17:31:03-05:00
[INFO] 2025-02-28T17:31:03-05:00
[INFO] 2025-02-28T17:31:03-05:00
[INFO] 2025-02-28T17:31:03-05:00
[INFO] 2025-02-28T17:31:03-05:00
[INFO] 2025-02-28T17:31:03-05:00 Digging deeper!                  https://www.velocidex.com
[INFO] 2025-02-28T17:31:03-05:00 This is Velociraptor 0.6.5-2 built on 2022-07-27T02:36:42+10:00 (795f9339)
[INFO] 2025-02-28T17:31:03-05:00 Generating keys please wait....
? Path to the logs directory. /opt/velociraptor/logs
? Where should i write the server config file? server.config.yaml
? Where should i write the client config file? client.config.yaml

┌──(user㉿kali)-[~]
└─$ la
.bash_logout      client.config.yaml  Documents   .gnupg         .mozilla  Public                      Templates    .xsession-errors
.bashrc           .config             Downloads   .ICEauthority  Music     raptor                      Videos       .xsession-errors.old
.bashrc.original  Desktop             .face       .java          Pictures  server.config.yaml          .wget-hsts   .zsh_history
.cache            .dmrc               .face.icon  .local         .profile  .sudo_as_admin_successful  .Xauthority  .zshrc

┌──(user㉿kali)-[~]
└─$ 
```



Welcome to Velociraptor!

Common tasks:

- Inspect the server's state
- Building an Offline Collector
- Write VQL notebooks
- View Server Configuration
- Customize this welcome screen

Or simply search for a client in the search bar above.

You can always get back to this welcome screen by clicking the little green reptile above!

2025-02-28T22:33:54Z