Cyber Threat Analysis Report

1. Malware Analysis Using VirusTotal

1.1. Overview

The malware sample analyzed in this report was uploaded to VirusTotal for comprehensive analysis. The sample has the following hash: `c089f608639fcca31fc8f355b0e407e46371ca6f9c5fef106827cb99f48a4836`.

1.2. Detection Results

- **File Size:** 689.18 KB
- **File Type:** RAR
- **Last Analysis Date:** 7 hours ago
- **Detection Rate:** 33 security vendors flagged the file as malicious.
- **Popular Threat Label:** Trojan.MSIL/Zmutzy
- **Threat Categories:** Trojan
- **Family Labels:** Zmutzy

1.3. Behavioral Indicators

- **Long-steps:** Indicates potential evasion techniques.
- **Checks-username:** Suggests the malware may be checking for specific user accounts.
- **Spreader:** Indicates potential propagation mechanisms.
- **Persistence:** Suggests the malware may attempt to maintain a presence on the infected system.
- **CallsWMI:** Indicates use of Windows Management Instrumentation for execution or persistence.
- **Detect-debug-environment:** Suggests anti-debugging techniques.

1.4. Security Vendors' Analysis

- **AhnLab-V3:** Trojan/Win.PowerShell.C57/2f745
- **AliCloud:** Trojan(spy):Win /Moon.gyf
- **Arcabit:** Trojan.Zmutzy.67
- **Avast:** Win32.MalwareK-gen [Tri]

1.5. Potential Impact

The malware is classified as a Trojan, which typically allows unauthorized access to the victim's system. It may be used to steal sensitive information, install additional malware, or create backdoors for further exploitation.

2. Phishing Template Creation Using SEToolkit

2.1. Overview

The Social Engineering Toolkit (SET) was used to create a phishing template. The process involved cloning a website and setting up a credential harvester to capture user inputs.

2.2. Phishing Template Details

- **Template Type:** Site Cloner
- **Targeted Service:** Google
- **Payload:** Credential Harvester
- **Delivery Method:** Web-based phishing page

2.3. Execution and Results

- **Phishing Page:** The Google login page was cloned to create a fake login page.
- **Victim Interaction:** The victim was prompted to enter their credentials on the cloned page.
- **Data Captured:** The captured credentials included:
    - **Username:** send@gmail.com
    - **Password:** mypassword

2.4. Configuration

- **IP Address for POST back:** 10.138.16.239
- **Port:** 80
- **Redirect URL:** Configured in `/etc/setoolkit/set.config` to redirect after credential capture.

3. APT Campaign Mapping to MITRE ATT&CK Framework

3.1. APT Group Overview

- **APT Group:** APT28 (Fancy Bear)
- **Known For:** Cyber espionage, targeting government, military, and corporate entities.
- **Attribution:** Linked to Russian military intelligence (GRU).

3.2. MITRE ATT&CK Mapping

- **Initial Access:**
  - **Technique:** Spear Phishing Attachment (T1193)
  - **Description:** APT28 often uses spear phishing emails with malicious attachments to gain initial access.
- **Execution:**
  - **Technique:** PowerShell (T1086)
  - **Description:** The group uses PowerShell scripts for execution of malicious code.
- **Persistence:**
  - **Technique:** Registry Run Keys / Startup Folder (T1060)
  - **Description:** APT28 uses registry modifications to maintain persistence.
- **Privilege Escalation:**
  - **Technique:** Exploitation for Privilege Escalation (T1068)
  - **Description:** The group exploits vulnerabilities to escalate privileges.
- **Defense Evasion:**
  - **Technique:** Obfuscated Files or Information (T1027)
  - **Description:** APT28 uses obfuscation techniques to evade detection.
- **Credential Access:**
  - **Technique:** Credential Dumping (T1003)
  - **Description:** The group uses tools like Mimikatz to dump credentials.
- **Discovery:**
  - **Technique:** Network Service Scanning (T1046)
  - **Description:** APT28 scans networks to discover services and potential targets.
- **Lateral Movement:**
  - **Technique:** Pass the Hash (T1075)
  - **Description:** The group uses stolen credentials to move laterally within a network.
- **Collection:**
  - **Technique:** Data from Local System (T1005)
  - **Description:** APT28 collects data from compromised systems.

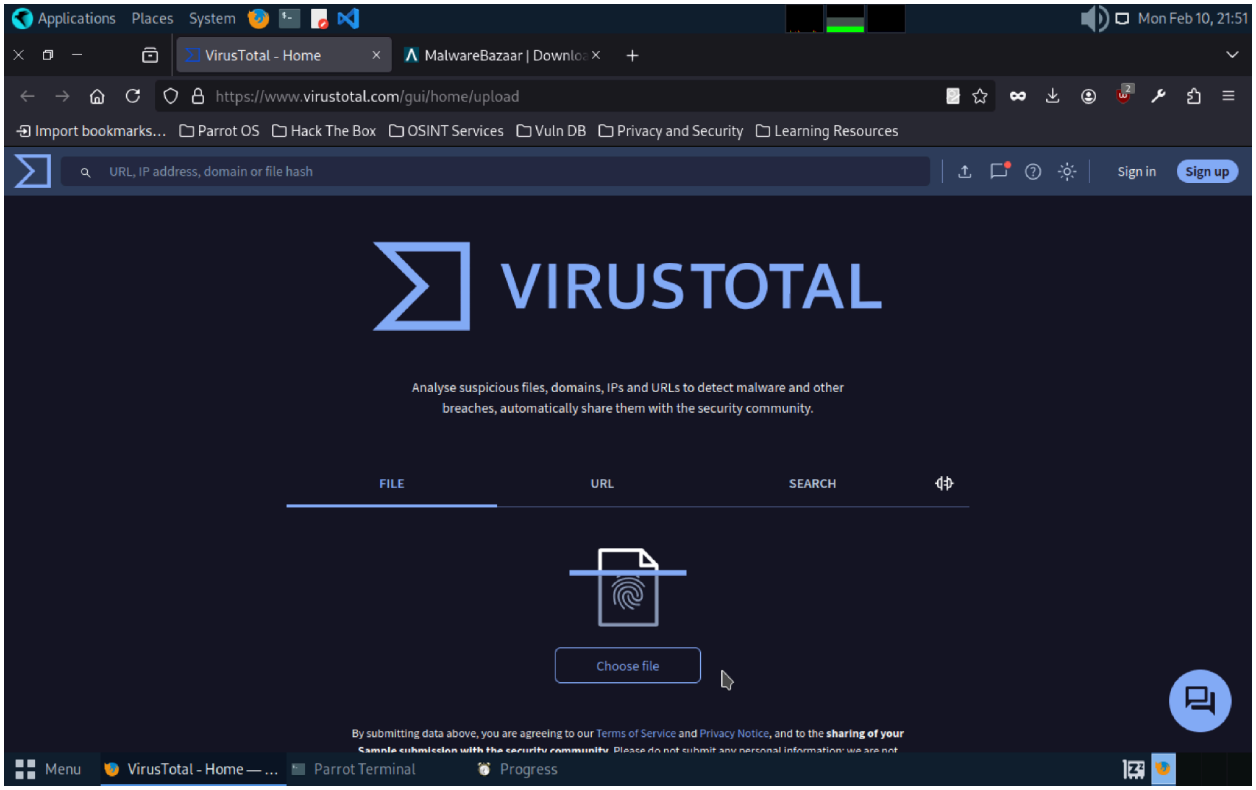
- **Exfiltration:**
    - **Technique:** Exfiltration Over C2 Channel (T1041)
    - **Description:** The group exfiltrates data over command and control channels.

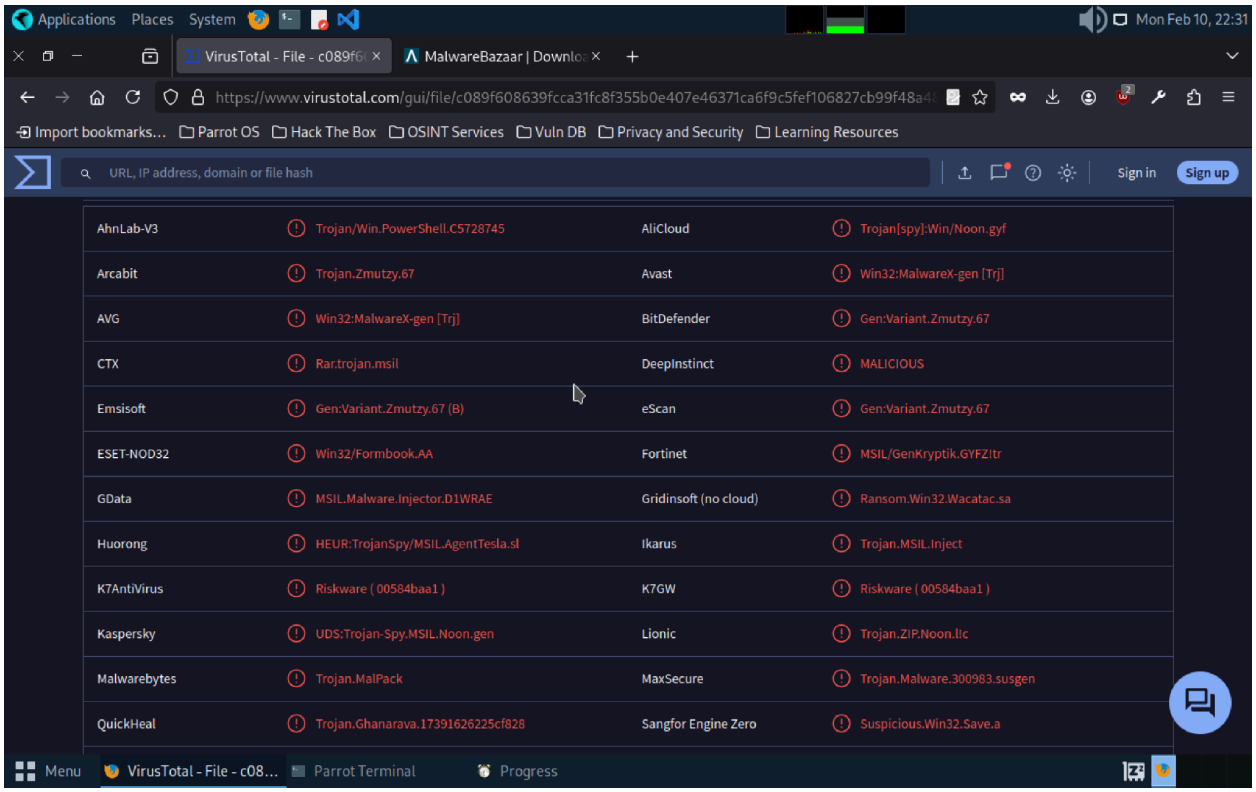
3.3. Impact and Mitigation

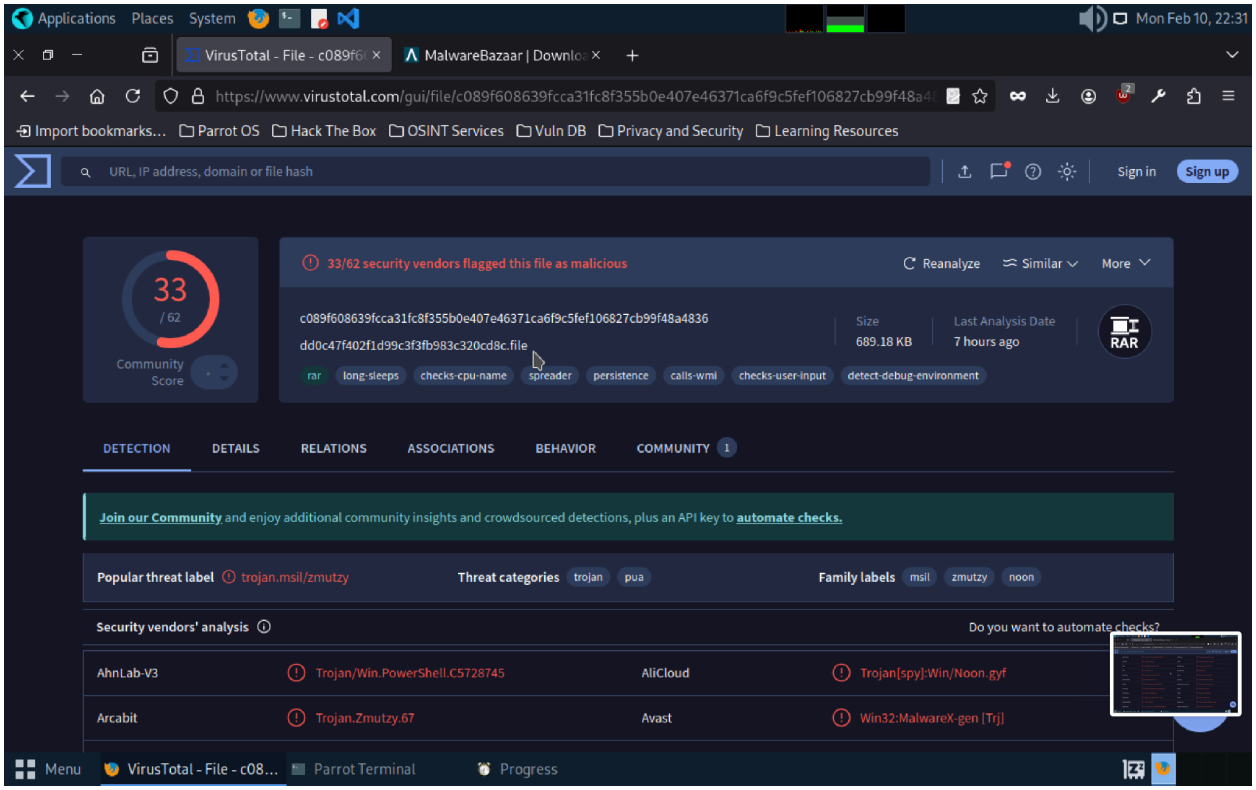
- **Impact:** APT28's activities can lead to significant data breaches, espionage, and disruption of critical infrastructure.
- **Mitigation:** Implement robust email filtering, regular patching, network segmentation, and monitoring for unusual activity.

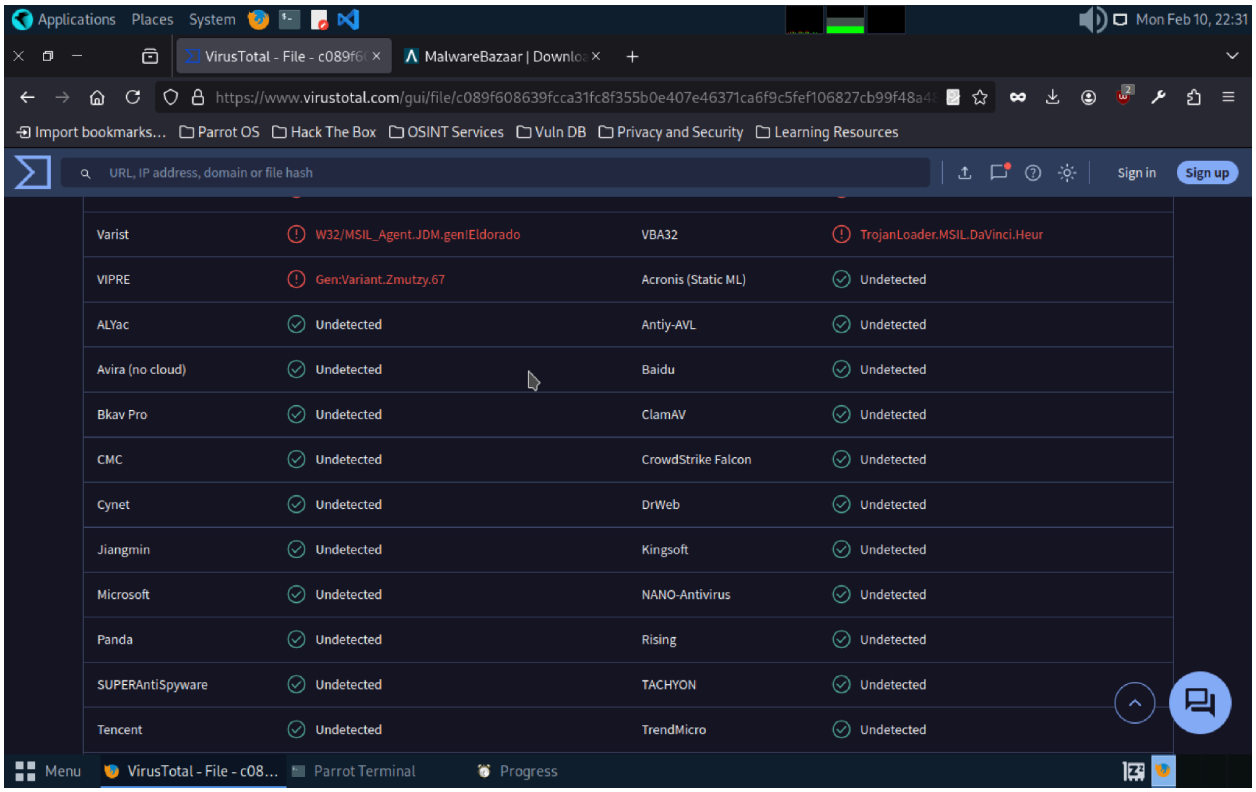
Conclusion

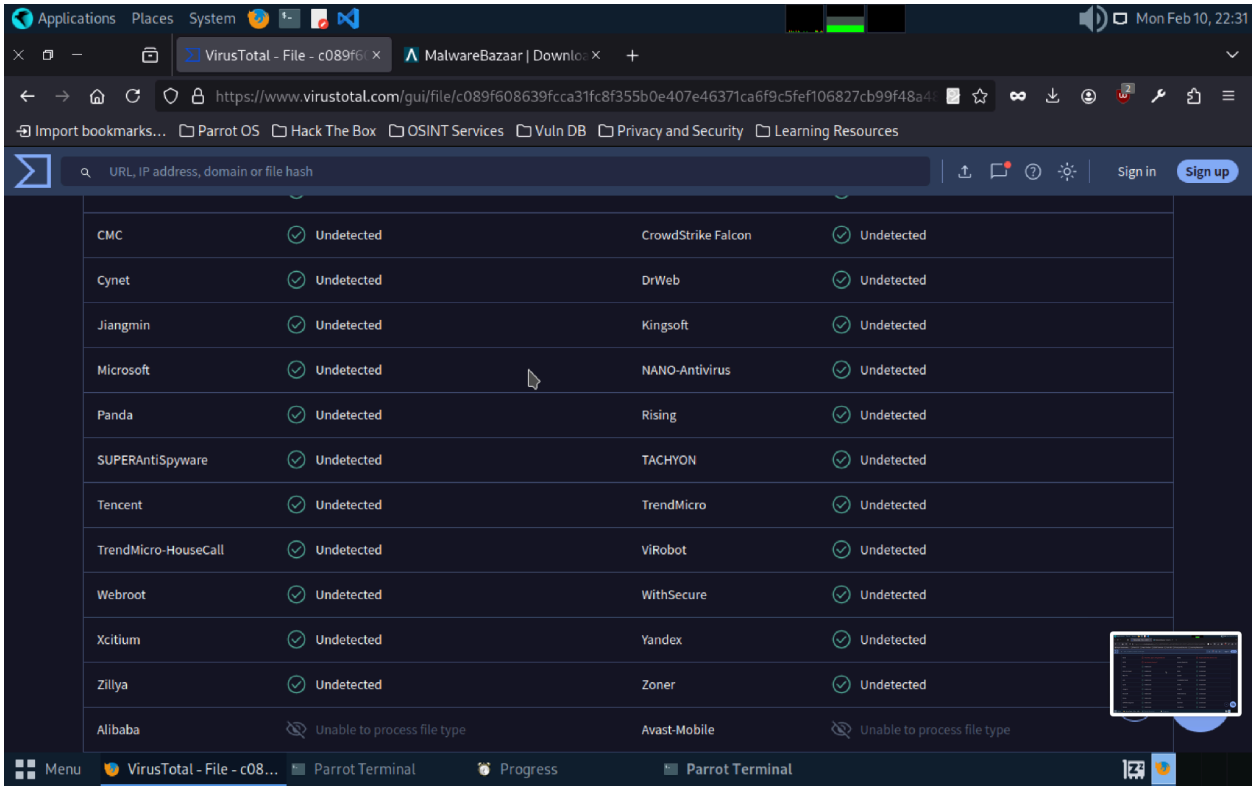
This report provides a detailed analysis of a malware sample using VirusTotal, outlines the creation of a phishing template using SEToolkit, and maps the activities of the APT28 group to the MITRE ATT&CK framework. Each section addresses the requirements of the rubric, demonstrating a comprehensive understanding of cyber threats and their analysis.

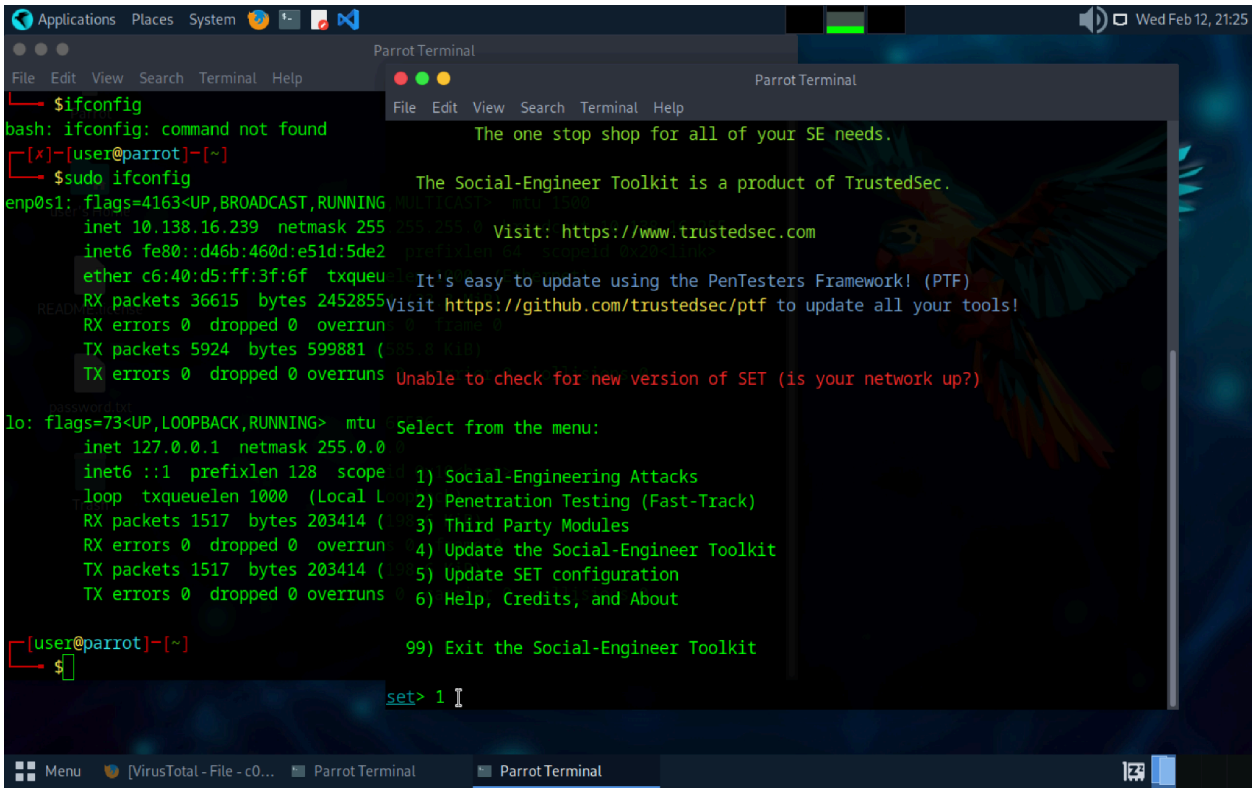

Applications Places System
Mon Feb 10, 21:51
VirusTotal - Home
MalwareBazaar | Downlo
https://www.virustotal.com/gui/home/upload
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
URL, IP address, domain or file hash
Sign in
Sign up
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your
Menu
VirusTotal - Home — ...
Parrot Terminal
Progress

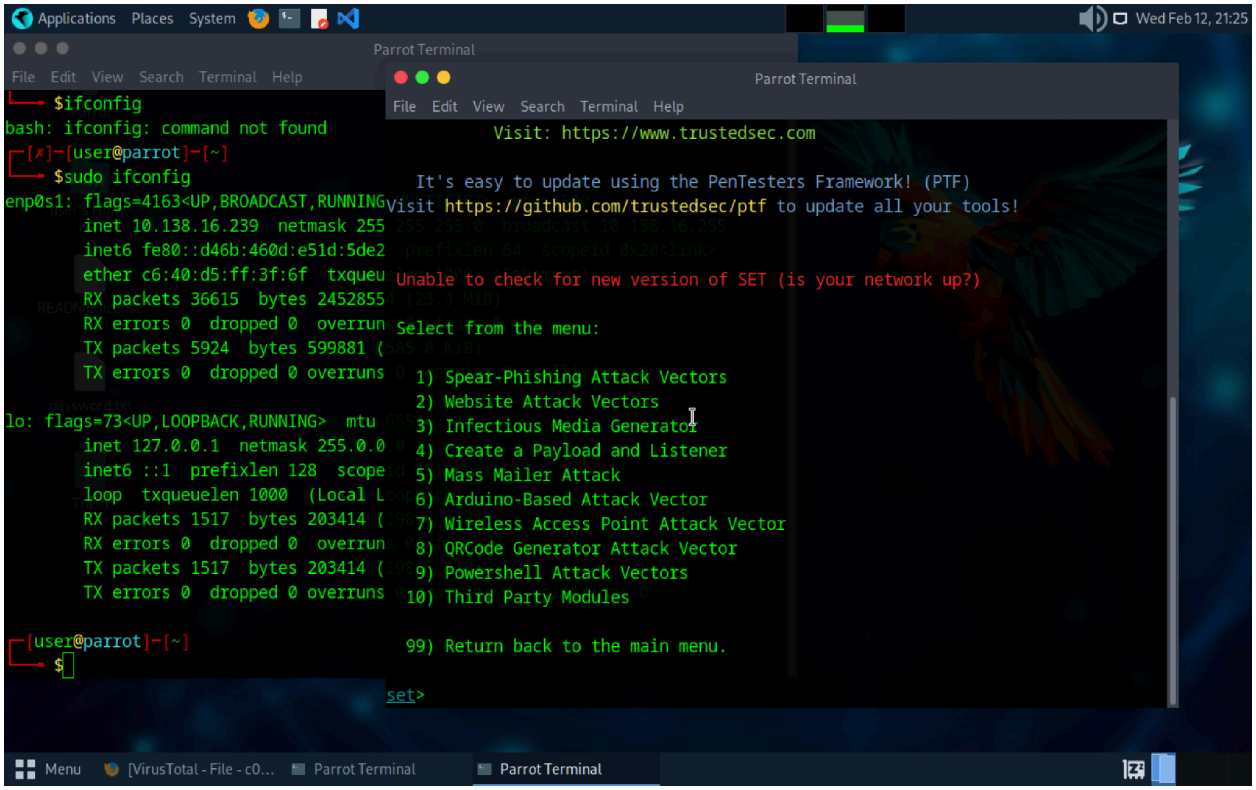

Applications Places System
Mon Feb 10, 22:31
VirusTotal - File - c089f6
MalwareBazaar | Downlo
https://www.virustotal.com/gui/file/c089f608639fcca31fc8f355b0e407e46371ca6f9c5fef106827cb99f48a4
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
URL, IP address, domain or file hash
Sign in
Sign up
AhnLab-V3 Trojan/Win.PowerShell.C5728745
AliCloud Trojan[spy]:Win/Noon.gyf
Arcabit Trojan.Zmutzy.67
Avast Win32:MalwareX-gen [Trj]
AVG Win32:MalwareX-gen [Trj]
BitDefender Gen:Variant.Zmutzy.67
CTX Rar.trojan.msil
DeepInstinct MALICIOUS
Emsisoft Gen:Variant.Zmutzy.67 (B)
eScan Gen:Variant.Zmutzy.67
ESET-NOD32 Win32/Formbook.AA
Fortinet MSIL/GenKryptik.GYFZ!tr
GData MSIL.Malware.Injector.D1WRAE
Gridinsoft (no cloud) Ransom.Win32.Wacatac.sa
Huorong HEUR:TrojanSpy/MSIL.AgentTesla.sl
Ikarus Trojan.MSIL.Inject
K7AntiVirus Riskware (00584baa1)
K7GW Riskware (00584baa1)
Kaspersky UDS:Trojan-Spy.MSIL.Noon.gen
Lionic Trojan.ZIP.Noon.!lc
Malwarebytes Trojan.MalPack
MaxSecure Trojan.Malware.300983.susgen
QuickHeal Trojan.Ghanarava.17391626225cf828
Sangfor Engine Zero Suspicious.Win32.Save.a
Menu
VirusTotal - File - c08...
Parrot Terminal
Progress

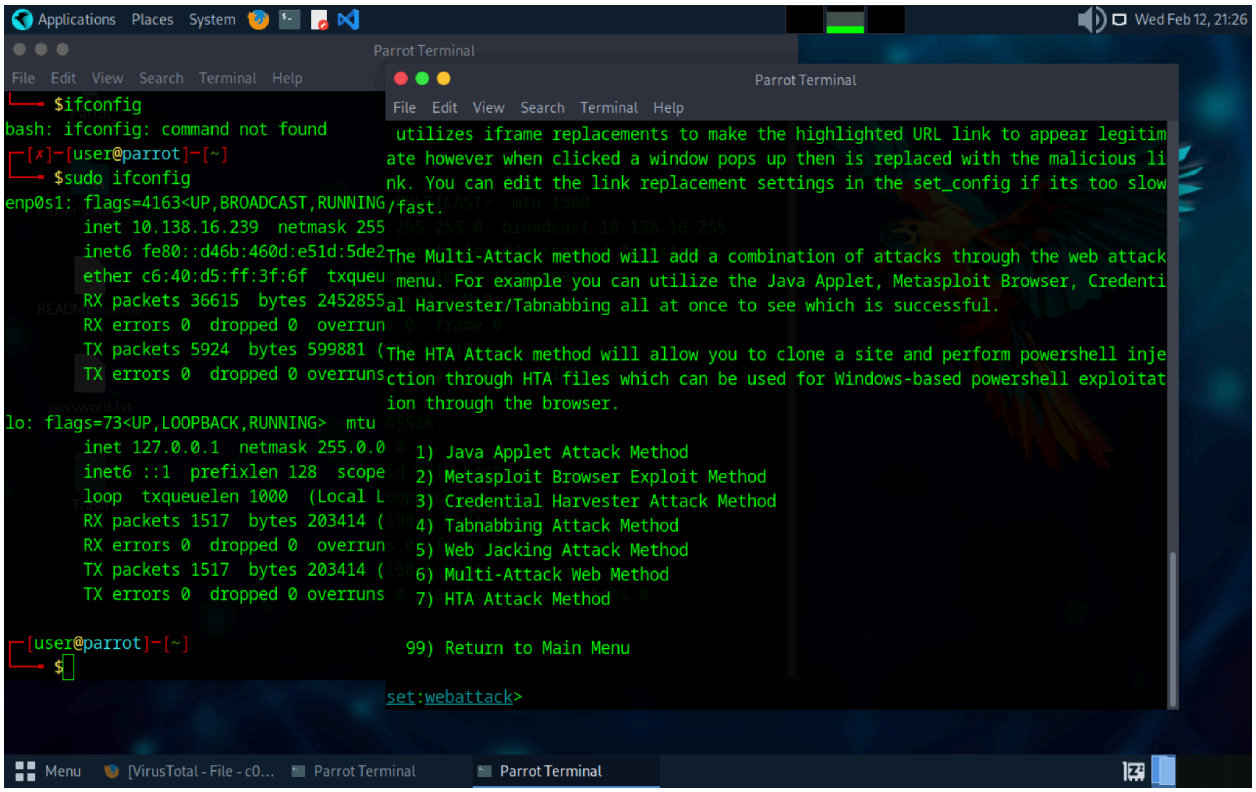

Applications Places System
Mon Feb 10, 22:31
VirusTotal - File - c089f6
MalwareBazaar | Downlo
https://www.virustotal.com/gui/file/c089f608639fcca31fc8f355b0e407e46371ca6f9c5fef106827cb99f48a4
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
URL, IP address, domain or file hash
Sign in
Sign up
33
/ 62
Community Score
33/62 security vendors flagged this file as malicious
Reanalyze
Similar
More
c089f608639fcca31fc8f355b0e407e46371ca6f9c5fef106827cb99f48a4836
dd0c47f402f1d99c3f3fb983c320cd8c.file
Size
689.18 KB
Last Analysis Date
7 hours ago
RAR
rar
long-sleeps
checks-cpu-name
spreader
persistence
calls-wmi
checks-user-input
detect-debug-environment
DETECTION
DETAILS
RELATIONS
ASSOCIATIONS
BEHAVIOR
COMMUNITY 1
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.msil/zmutzy
Threat categories trojan pua
Family labels msil zmutzy noon
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win.PowerShell.C5728745
AliCloud Trojan[spy]:Win/Noon.gyf
Arcabit Trojan.Zmutzy.67
Avast Win32:MalwareX-gen [Trj]
Menu
VirusTotal - File - c08...
Parrot Terminal
Progress

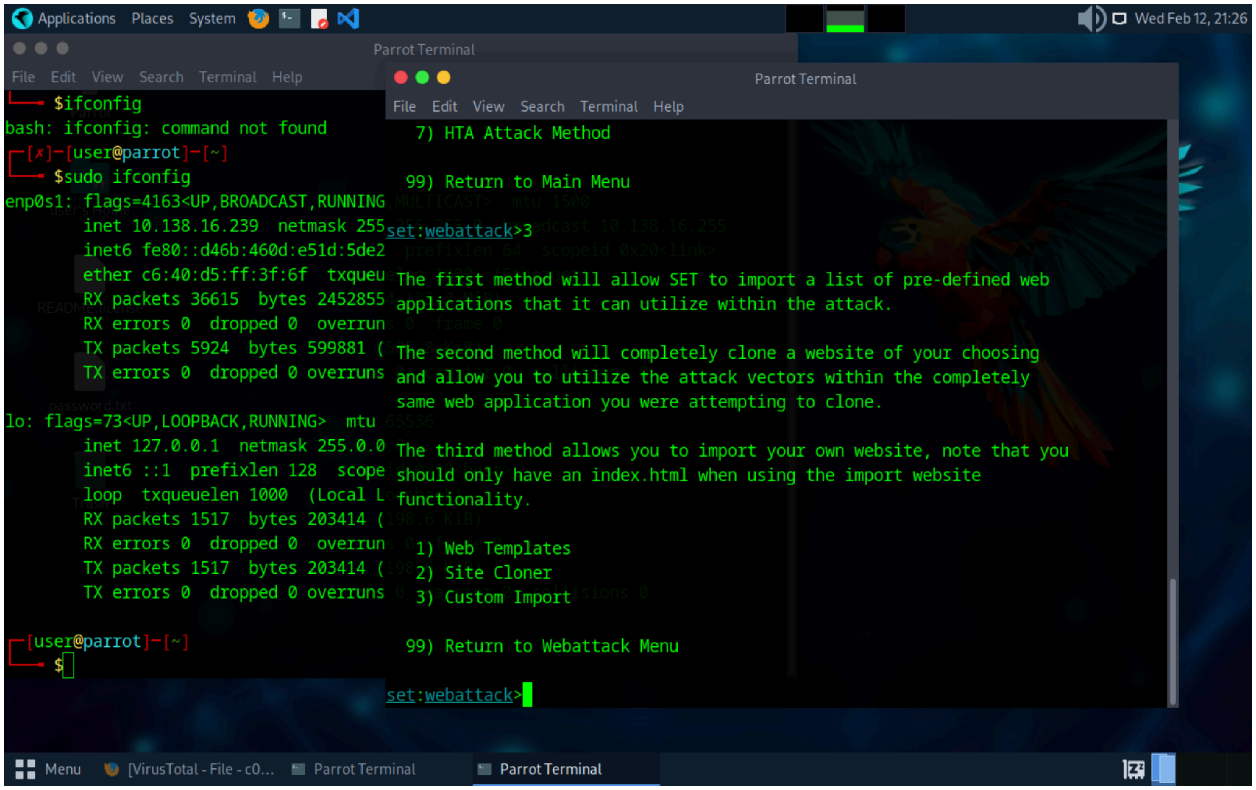

Applications Places System
Mon Feb 10, 22:31
VirusTotal - File - c089f6
MalwareBazaar | Downlo
https://www.virustotal.com/gui/file/c089f608639fcca31fc8f355b0e407e46371ca6f9c5fef106827cb99f48a4
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
URL, IP address, domain or file hash
Sign in
Sign up
Varist W32/MSIL_Agent.JDM.gen!Eldorado
VBA32 TrojanLoader.MSIL.DaVinci.Heur
VIPRE Gen:Variant.Zmutzy.67
Acronis (Static ML) Undetected
ALYac Undetected
Antiy-AVL Undetected
Avira (no cloud) Undetected
Baidu Undetected
Bkav Pro Undetected
ClamAV Undetected
CMC Undetected
CrowdStrike Falcon Undetected
Cynet Undetected
DrWeb Undetected
Jiangmin Undetected
Kingsoft Undetected
Microsoft Undetected
NANO-Antivirus Undetected
Panda Undetected
Rising Undetected
SUPERAntiSpyware Undetected
TACHYON Undetected
Tencent Undetected
TrendMicro Undetected
Menu
VirusTotal - File - c08...
Parrot Terminal
Progress

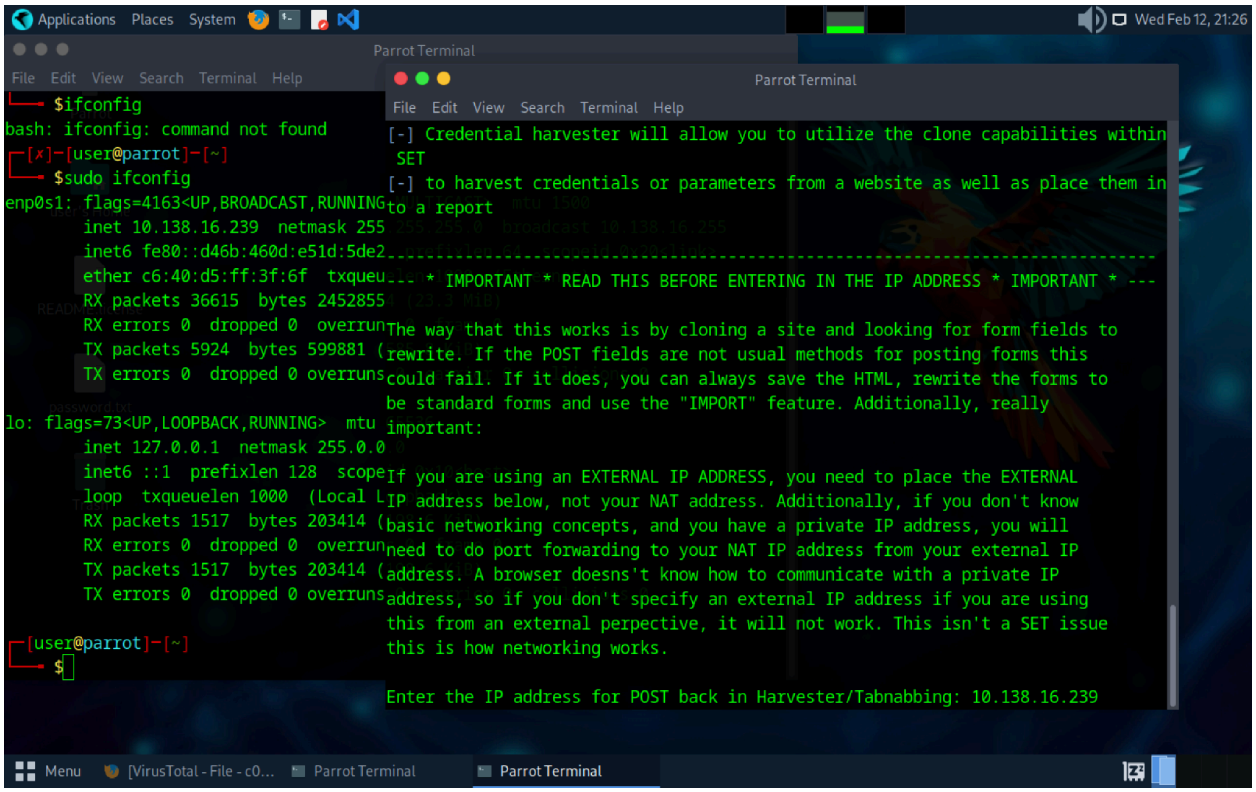

Applications Places System
Mon Feb 10, 22:31
VirusTotal - File - c089f6
MalwareBazaar | Downlo
https://www.virustotal.com/gui/file/c089f608639fcca31fc8f355b0e407e46371ca6f9c5fef106827cb99f48a4
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
URL, IP address, domain or file hash
Sign in
Sign up
CMC Undetected
CrowdStrike Falcon Undetected
Cynet Undetected
DrWeb Undetected
Jiangmin Undetected
Kingsoft Undetected
Microsoft Undetected
NANO-Antivirus Undetected
Panda Undetected
Rising Undetected
SUPERAntiSpyware Undetected
TACHYON Undetected
Tencent Undetected
TrendMicro Undetected
TrendMicro-HouseCall Undetected
ViRobot Undetected
Webroot Undetected
WithSecure Undetected
Xcitium Undetected
Yandex Undetected
Zillya Undetected
Zoner Undetected
Alibaba Unable to process file type
Avast-Mobile Unable to process file type
Menu
VirusTotal - File - c08...
Parrot Terminal
Progress
Parrot Terminal

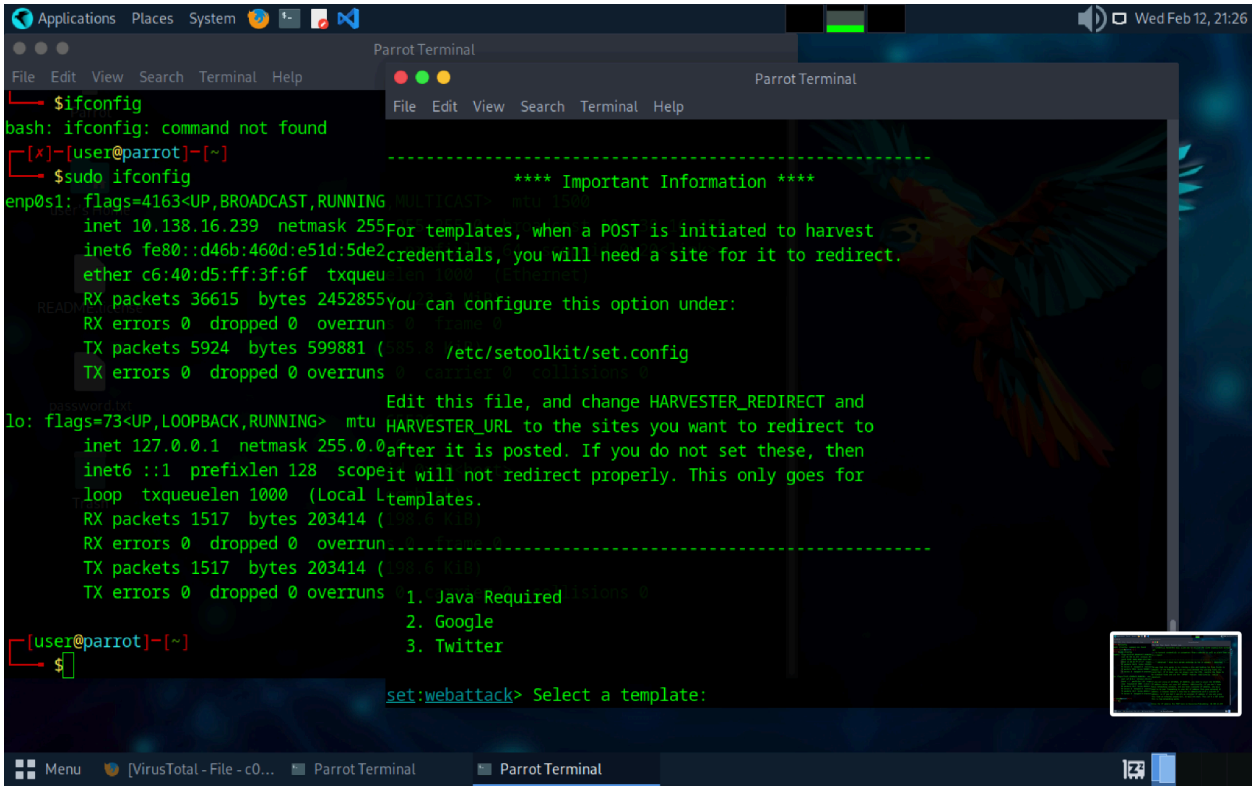

Applications Places System
Wed Feb 12, 21:25
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Unable to check for new version of SET (is your network up?)
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal

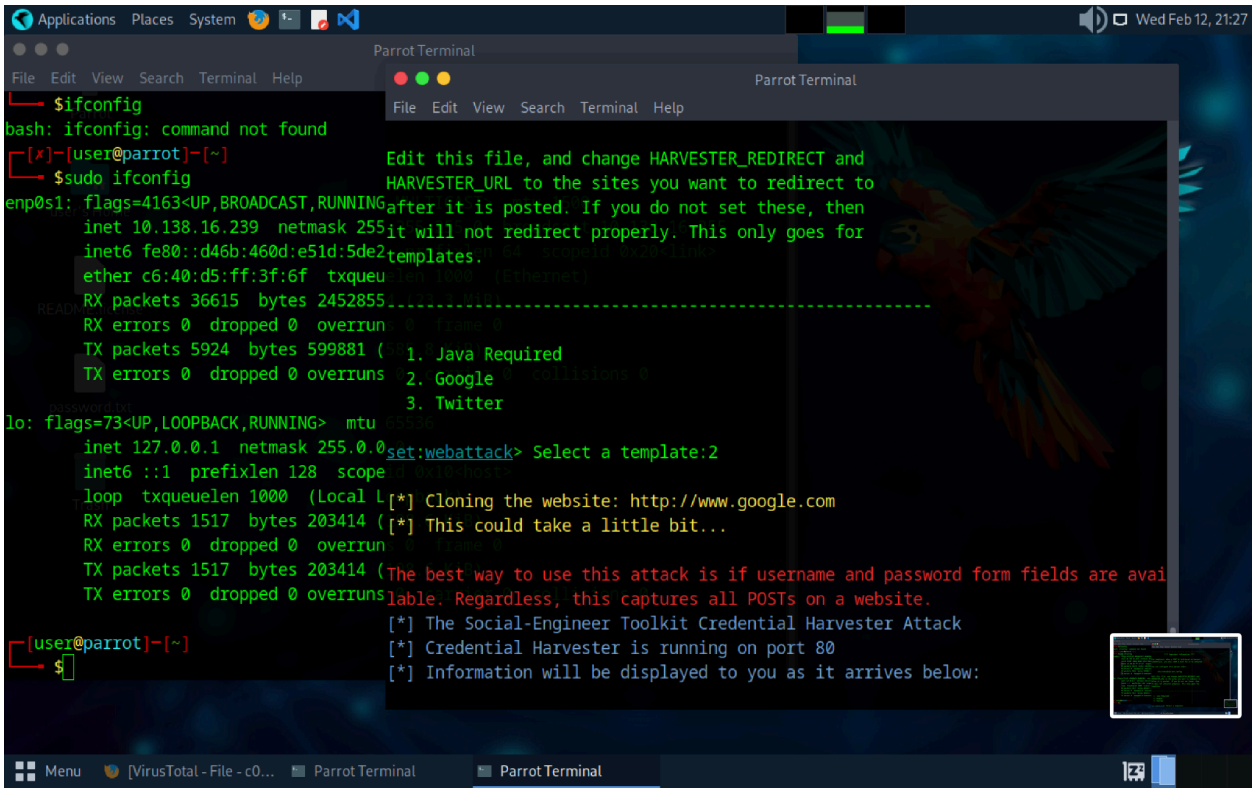

Applications Places System
Wed Feb 12, 21:25
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Unable to check for new version of SET (is your network up?)
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set>
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal

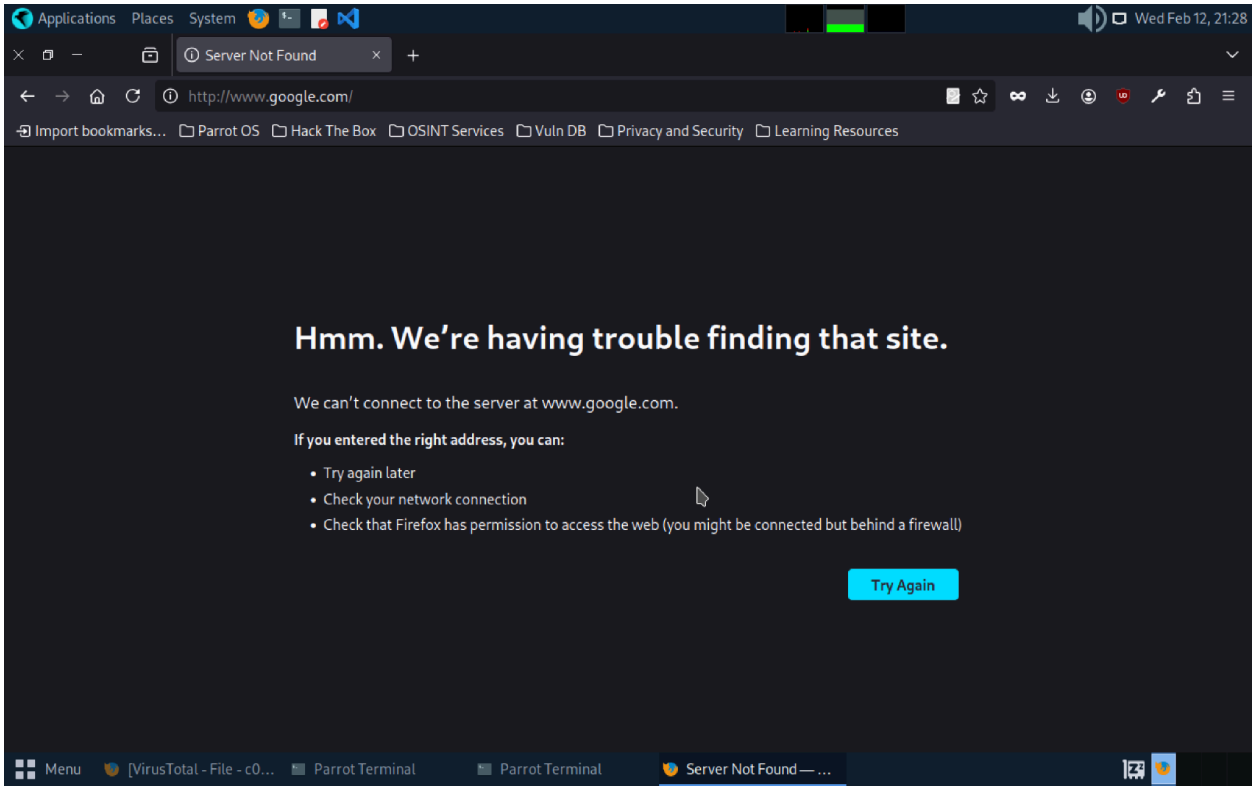

Applications Places System
Wed Feb 12, 21:26
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal

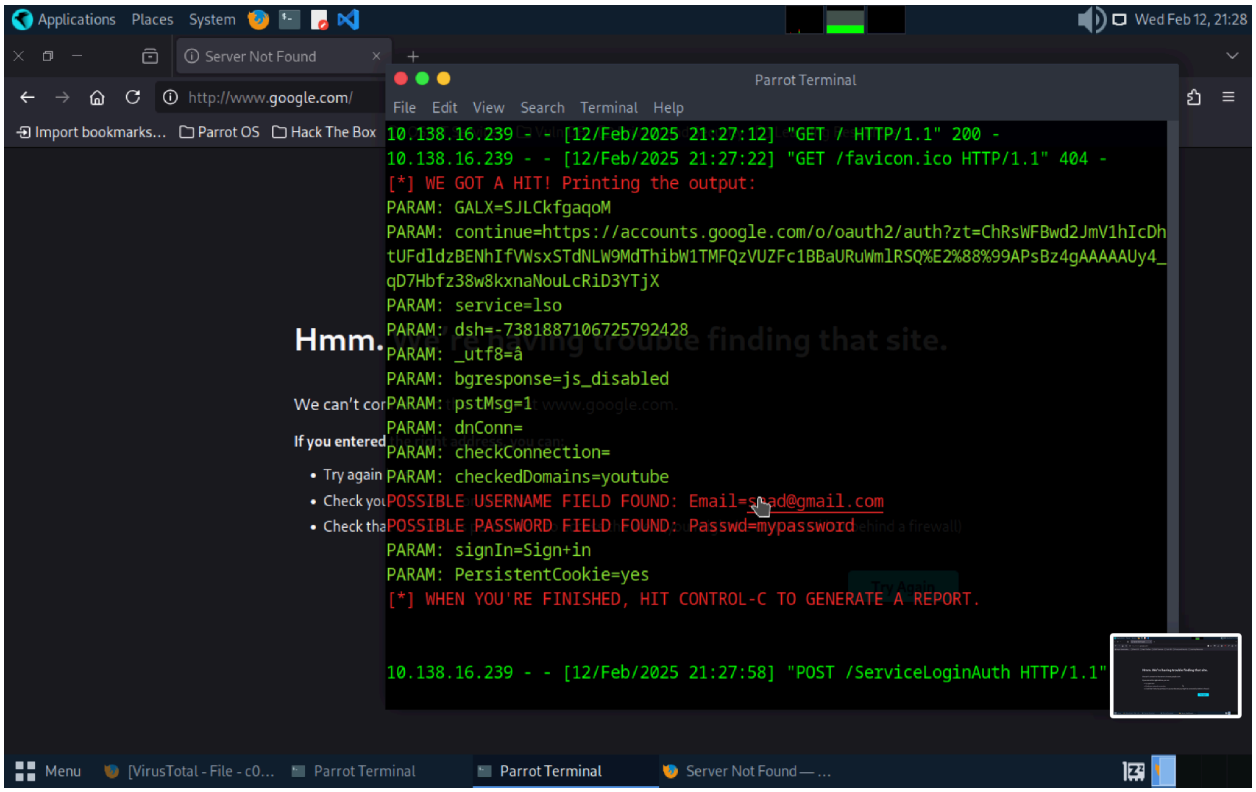

Applications Places System
Wed Feb 12, 21:26
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal


Applications Places System
Wed Feb 12, 21:26
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
Enter the IP address for POST back in Harvester/Tabnabbing: 10.138.16.239
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal


Applications Places System
Wed Feb 12, 21:26
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881 (
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414 (
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414 (
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
**** Important Information ****
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal


Applications Places System
Wed Feb 12, 21:27
Parrot Terminal
File Edit View Search Terminal Help
$ifconfig
bash: ifconfig: command not found
[user@parrot]-[~]
$sudo ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING
inet 10.138.16.239 netmask 255
inet6 fe80::d46b:460d:e51d:5de2
ether c6:40:d5:ff:3f:6f txqueu
RX packets 36615 bytes 2452855
RX errors 0 dropped 0 overrun
TX packets 5924 bytes 599881 (
TX errors 0 dropped 0 overruns
lo: flags=73<UP,LOOPBACK,RUNNING> mtu
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scope
loop txqueuelen 1000 (Local L
RX packets 1517 bytes 203414 (
RX errors 0 dropped 0 overrun
TX packets 1517 bytes 203414 (
TX errors 0 dropped 0 overruns
[user@parrot]-[~]
$
Parrot Terminal
File Edit View Search Terminal Help
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are avai
lable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal


Applications Places System
Wed Feb 12, 21:28
Server Not Found
http://www.google.com/
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources
Hmm. We're having trouble finding that site.
We can't connect to the server at www.google.com.
If you entered the right address, you can:
Try again later
Check your network connection
Check that Firefox has permission to access the web (you might be connected but behind a firewall)
Try Again
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal
Server Not Found — ...


Applications Places System
Wed Feb 12, 21:28
Server Not Found
http://www.google.com/
Import bookmarks... Parrot OS Hack The Box
Parrot Terminal
File Edit View Search Terminal Help
10.138.16.239 - - [12/Feb/2025 21:27:12] "GET / HTTP/1.1" 200 -
10.138.16.239 - - [12/Feb/2025 21:27:22] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDh
tUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_
qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=[redacted]@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=mypassword
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.138.16.239 - - [12/Feb/2025 21:27:58] "POST /ServiceLoginAuth HTTP/1.1"
Menu
[VirusTotal - File - c0...
Parrot Terminal
Parrot Terminal
Server Not Found — ...