

Parrot Terminal

```
File Edit View Search Terminal Help
cat: http.log: No such file or directory
cat: dns.log: No such file or directory
[user@parrot]~]
└─ $cd /usr/local/zeek/logs/current/
bash: cd: /usr/local/zeek/logs/current/: No such file or directory
[x]~[user@parrot]~]
└─ $cat http.log | less
cat: http.log: No such file or directory
[user@parrot]~]
└─ $cd /usr/local/zeek/logs/current/
bash: cd: /usr/local/zeek/logs/current/: No such file or directory
[x]~[user@parrot]~]
└─ $sudo nmap -sS 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-21 21:49 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored state
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
[user@parrot]~]
└─ $curl http://testmyids.com
uid=0(root) gid=0(root) groups=0(root)
[user@parrot]~]
bash: : command not found
```

Parrot Terminal

File Edit View Search Terminal Help

tion | © 2019
Acunetix Ltd

</div>

user's Home

<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">

<p style="padding-left:5%;padding-right:5%">Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.</p>

</div> Trash

</div>

</body>

<!-- InstanceEnd --></html>

[user@parrot]~

\$ cd /usr/local/zeek/logs/current/
cat http.log | less
cat dns.log | less
bash: cd: /usr/local/zeek/logs/current/: No such file or directory

bash: .. command not found
bash: .. command not found

Threat_Analysis.md

bash: SOC_Fundamentals_Project/: No such file or directory

bash: .. command not found
bash: .. command not found


```
File Edit View Search Terminal Help
<div id="search">
  <form action="search.php?test=query" method="post">
    <label>search art</label>
    <input name="searchFor" type="text" size="10">
    <input name="goButton" type="submit" value="go">
  </form>
</div>
<div id="sectionLinks">
  <ul>
    <li><a href="categories.php">Browse categories</a></li>
    <li><a href="artists.php">Browse artists</a></li>
    <li><a href="cart.php">Your cart</a></li>
    <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </li>
  </ul>
</div>
<div class="relatedLinks">
  <h3>Links</h3>
  <ul>
    <li><a href="http://www.acunetix.com">Security art</a></li>
    <li><a href="https://www.acunetix.com/vulnerability-scanner/php-securi
  </ul>
</div>
```

Parrot Terminal

```
File Edit View Search Terminal Help
hp">your cart</a> |
    <a href="guestbook.php">guestbook</a> |
    <a href="AJAX/index.php">AJAX Demo</a>
    </td>
    <td align="right">
        </td>
    </tr></table>
</div>
</div>
<!-- end masthead --&gt;

<!-- begin content --&gt;
<!-- InstanceBeginEditable name="content_rgn" --&gt;
&lt;div id="content"&gt;
    &lt;h2 id="pageName"&gt;welcome to our page&lt;/h2&gt;
    &lt;div class="story"&gt;
        &lt;h3&gt;Test site for Acunetix WVS.&lt;/h3&gt;
    &lt;/div&gt;
&lt;/div&gt;
<!-- InstanceEndEditable --&gt;
<!--end content --&gt;

&lt;div id="navBar"&gt;
    &lt;div id="search"&gt;</pre>

Parrot Terminal



```
[root@parrot] ~[user]
[]#SOC_Fundamentals_Project/
[]-- SOC_Roles.md
[]-- Monitoring_Tool_Setup.md
[]-- Screenshots/
[]-- Threat_Analysis.md
bash: SOC_Fundamentals_Project/: No such file or directory
bash: : command not found
```


```

Parrot Terminal

```
File Edit View Search Terminal Help
document.MM_pgW=innerWidth, document.MM_pgH=innerHeight, onresize=MM_reloadPage; } }

else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
user's Home
MM_reloadPage(true);
//-->
</script>
e README.license
</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
    <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
    <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
    <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr><td align="left">
            <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        </td></tr></table>
    </div>
</div>
<div id="contentLayer" style="position:absolute; top:0; left:0; width:100%; height:100%; background-color:white; z-index:0">
<div id="content">
<!-- InstanceBegin --></html>
[root@parrot]~[/home/user]
  #SOC_Fundamentals_Project/
    SOC_Roles.md
    Screenshots/
      dns_log.png
      Threat_Analysis.md
bash: command not found
bash: command not found
bash: command not found
bash: command not found
```

File Edit View Search Terminal Help

```
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
[x]-(user@parrot)-[~]
$ curl http://testphp.vulnweb.com
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { // reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW.innerWidth; document.MM_pgH.innerHeight; onresize=MM_reloadP
```

Parrot Terminal

File Edit View Search Terminal Help

```
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: This is not a real s
hop. This is an example PHP application, which is intentionally vulnerable to we
b attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your web site. You can use it to test other tools and your manual hacking skills as well.
Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.</p>
</div>
</div>
</body>
<!-- InstanceEnd --></html>
[user@parrot]~
$ping google.com
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+p capability or setuid?
[x]~[user@parrot]~
$curl http://testphp.vulnweb.com
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

The screenshot shows a terminal window titled "Parrot Terminal" with a dark theme. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content displays a warning message from a PHP application about web vulnerabilities, followed by a user's terminal session. The user tries to ping "google.com" and curl a URL, both of which fail due to permission issues ("Operation not permitted" and "missing cap_net_raw+p capability or setuid?"). The background of the terminal window shows a file tree for a "SOC Fundamentals Project" containing files like "README.license", "SOC_Fundamentals_Project/", "SOC_Roles.md", "Monitoring_Tool_Setup.md", "Screenshots/", "zeek_running.png", "http_log.png", "dns_log.png", "alert1_nmap.png", "alert2_ids.png", and "Threat_Analysis.md".

Parrot Terminal

```
File Edit View Search Terminal Help
</ul>
</div>
<div id="advert">
<p>User's Home
    <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">
        <!-- InstanceEnd --></html>
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high" pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>
    </object>
</p>
</div>
</div> Trash
<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | <a href="/Mod_Rewrite_Shop/">Shop</a> | <a href="/hpp/">HTTP Parameter Pollution</a> | &copy;2019
    Acunetix Ltd
</div>
```

Parrot Terminal

```
File Edit View Search Terminal Help
<input name="go" type="submit" value="go">
</form>
</div>
<div id="sectionLinks">
    <ul>
        <li><a href="categories.php">Browse categories</a></li>
        <li><a href="artists.php">Browse artists</a></li>
        <li><a href="cart.php">Your cart</a></li>
        <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
        <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
</div>
<div class="relatedLinks">
    <h3>Links</h3>
    <ul>
        <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
    </ul>
</div>
```

Parrot

README license

user's Home

Screenshots/

- zeek_running.png
- http_log.png
- dns_log.png
- alert1_nmap.png
- alert2_ids.png

bash: : command not found

Parrot Terminal

```
File Edit View Search Terminal Help
    <a href="AJAX/index.php">AJAX Demo</a>
</td>
<td align="right">
    </td>
</tr></table>
</div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
    <h2 id="pageName">welcome to our page</h2>
    <div class="story">
        <h3>Test site for Acunetix WVS.</h3>
    </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
    <div id="search">
        <form action="search.php?test=query" method="post">
            <label>search art</label>
    </form>
</div>
<div id="links">
    <ul>
        <li><a href="#">Home</a></li>
        <li><a href="#">About</a></li>
        <li><a href="#">Services</a></li>
        <li><a href="#">Contact</a></li>
    </ul>
</div>
<div id="logos">
    <img alt="Logos for various security tools: Zeek, Nmap, Wireshark, and Snort." data-bbox="180 100 350 250"/>
</div>
<div id="social">
    <ul>
        <li><a href="#">Facebook</a></li>
        <li><a href="#">Twitter</a></li>
        <li><a href="#">LinkedIn</a></li>
    </ul>
</div>
<div id="bottom">
    <p>Parrot OS - The Art of Security</p>
</div>
```

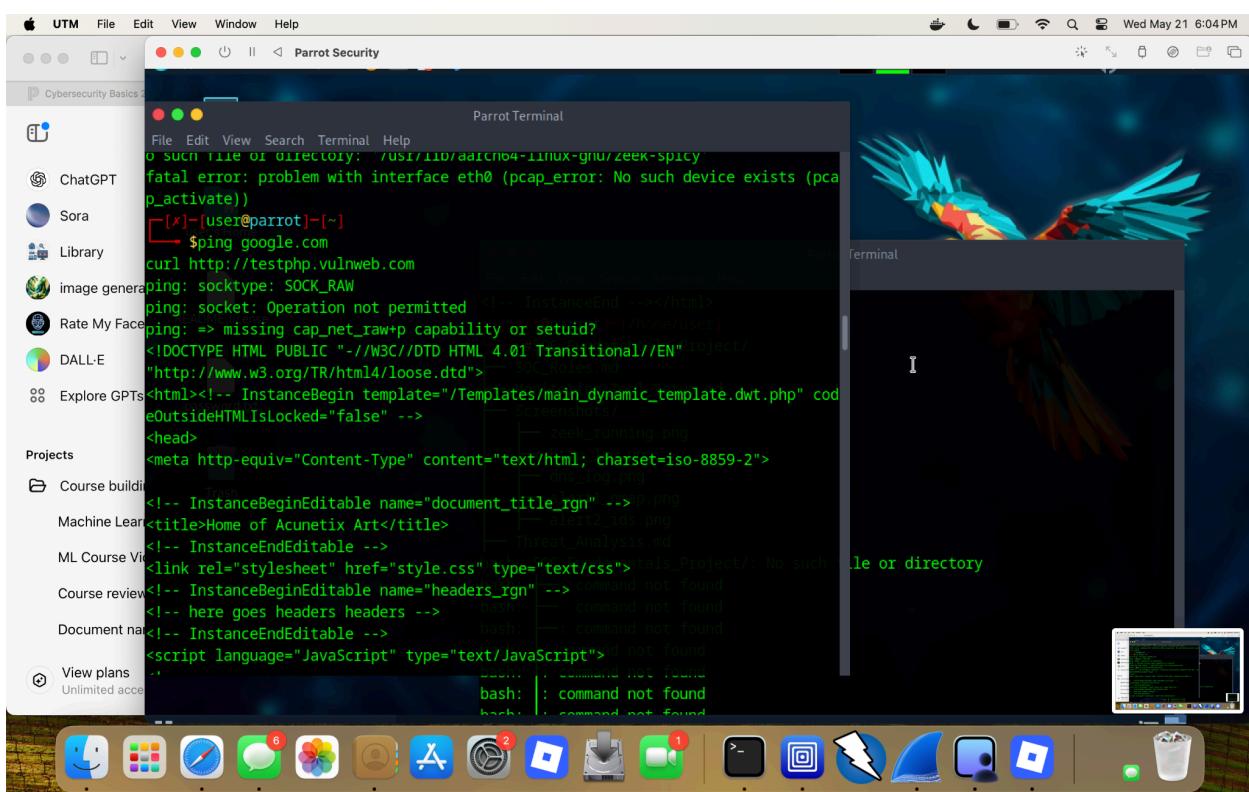
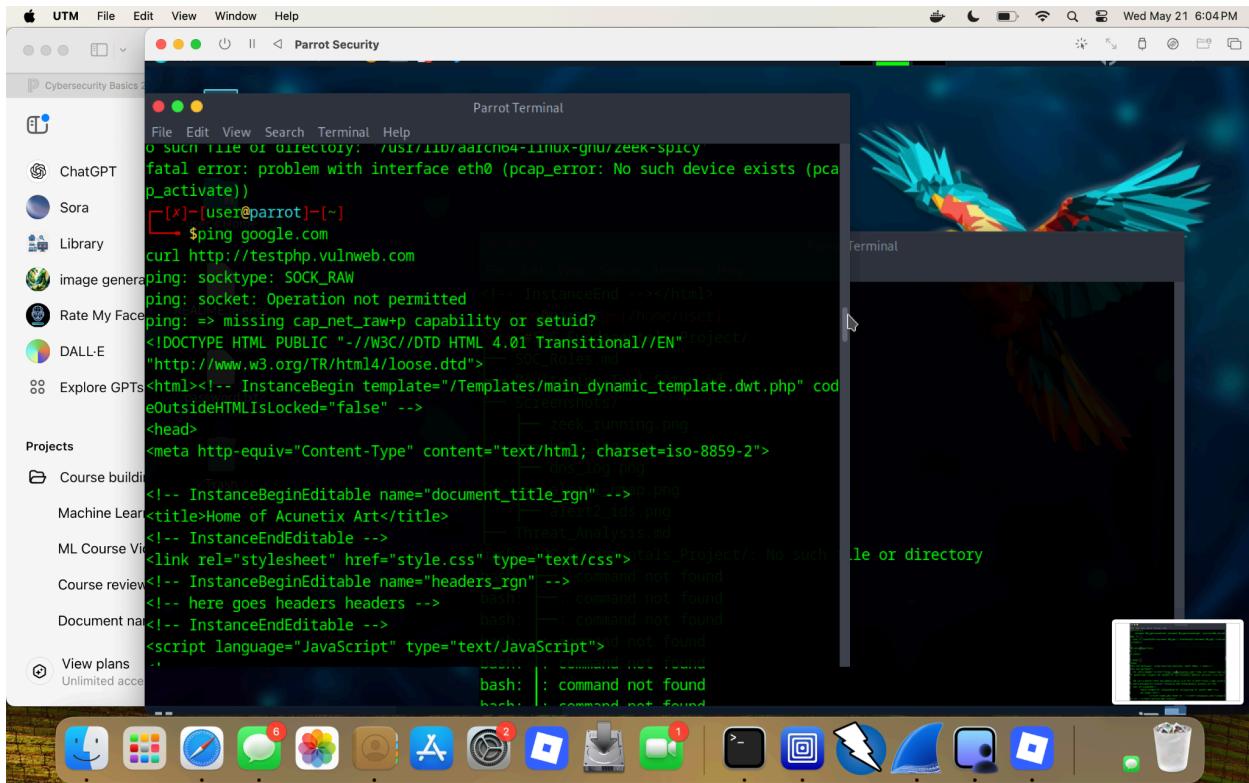
File Edit View Search Terminal Help

```
<!-- InstanceEnd --></html>
-[root@parrot]~[~/home/user]
--> #SOC_Fundamentals_Project/
--> SOC_Roles.md
--> Monitoring_Tool_Setup.md
--> Screenshots/
-->   zeek_running.png
-->   http_log.png
-->   dns_log.png
-->   alert1_nmap.png
-->   alert2_ids.png
--> Threat_Analysis.md
bash: SOC_Fundamentals_Project/: No such file or directory
bash: : command not found
```

File Edit View Search Terminal Help

```
ion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }
} else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location
.reload();
}
aMM_reloadPage(true);
//-->
e</script>

</head>
s<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
    <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
    <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acuneti
x.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
    <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
            <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">category
es</a> | <a href="artists.php">artists
            </td>
        </tr>
    </table>
</div>
<div id="contentArea">
<h2>Acunetix Web Vulnerability Scanner</h2>
<h3>Introduction</h3>
<p>This is a demonstration site for the Acunetix Web Vulnerability Scanner. It contains several known vulnerabilities for testing purposes. Please use it responsibly and ethically. No such
vulnerabilities should be found in real-world applications. The scanner is designed to identify and report on various types of web application vulnerabilities, including SQL injection, XSS, CSRF, and more. It uses a combination of static analysis and dynamic testing to provide comprehensive coverage. The results are presented in an easy-to-understand format, allowing users to quickly identify and fix issues in their own code. The scanner is available as a free trial version, which can be downloaded from the Acunetix website. It is also available as a paid commercial product, which provides additional features and support. The scanner is used by many organizations to help them identify and fix security vulnerabilities in their web applications. It is a valuable tool for anyone who wants to ensure the security of their web applications.
<h3>How to Use</h3>
<ol>
<li>1. Download and install the Acunetix Web Vulnerability Scanner</li>
<li>2. Configure the scanner to point to your web application</li>
<li>3. Run the scanner and review the results</li>
<li>4. Fix the identified vulnerabilities</li>
</ol>
<h3>Conclusion</h3>
<p>The Acunetix Web Vulnerability Scanner is a powerful tool for identifying and fixing security vulnerabilities in web applications. It is easy to use and provides comprehensive coverage of common web application vulnerabilities. By using the scanner, organizations can help ensure the security of their web applications and protect their users from potential threats. The scanner is available as a free trial version, which can be downloaded from the Acunetix website. It is also available as a paid commercial product, which provides additional features and support. The scanner is used by many organizations to help them identify and fix security vulnerabilities in their web applications. It is a valuable tool for anyone who wants to ensure the security of their web applications.</p>
</div>
</body>
```



Parrot Terminal

```
File Edit View Search Terminal Help
o such file or directory: /usr/lib/aarch64-linux-gnu/zeek-spicy
fatal error: problem with interface eth0 (pcap_error: No such device exists (pcap_activate))
[x]-[user@parrot]-
$ ping google.com
curl http://testphp.vulnweb.com
ping: socktype: SOCK_RAW
ping: socket: Operation not permitted
ping: => missing cap_net_raw+rp capability or setuid?
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" cod
eOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
..
```

File Edit View Search Terminal Help

```
<!-- InstanceEnd --></html>
[home/user]
#SOC_Fundamentals_Project/
SOC_Roles.md
Screenshots/
--> zeek_running.png
--> dns_log.png
--> alert1_nmap.png
--> alert2_ids.png
Threat_Analysis.md
trash: SOC_Fundamentals_Project/: No such file or directory
bash: command not found
```

```
File Edit View Search Terminal Help  
ease The following signatures couldn't be verified because the public key is no  
t available: NO_PUBKEY 7A8286AF0E81EE4A  
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory-backports/InRelease  
The following signatures couldn't be verified because the public key is not avai  
lable: NO_PUBKEY 7A8286AF0E81EE4A  
W: Some index files failed to download. They have been ignored, or old ones used  
instead.  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
zeek is already the newest version (5.1.1-0parrot1).  
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.  
[user@parrot]~  
└─$ sudo apt install zeek -y  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
zeek is already the newest version (5.1.1-0parrot1).  
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.  
[user@parrot]~  
└─$ sudo zeek -i eth0  
[warning] invalid plugin base directory /usr/lib/aarch64-linux-gnu/zeek-spicy: N  
o such file or directory: '/usr/lib/aarch64-linux-gnu/zeek-spicy'  
fatal error: problem with interface eth0 (pcap_error: No such device exists (pca
```

Parrot Terminal

File Edit View Search Terminal Help

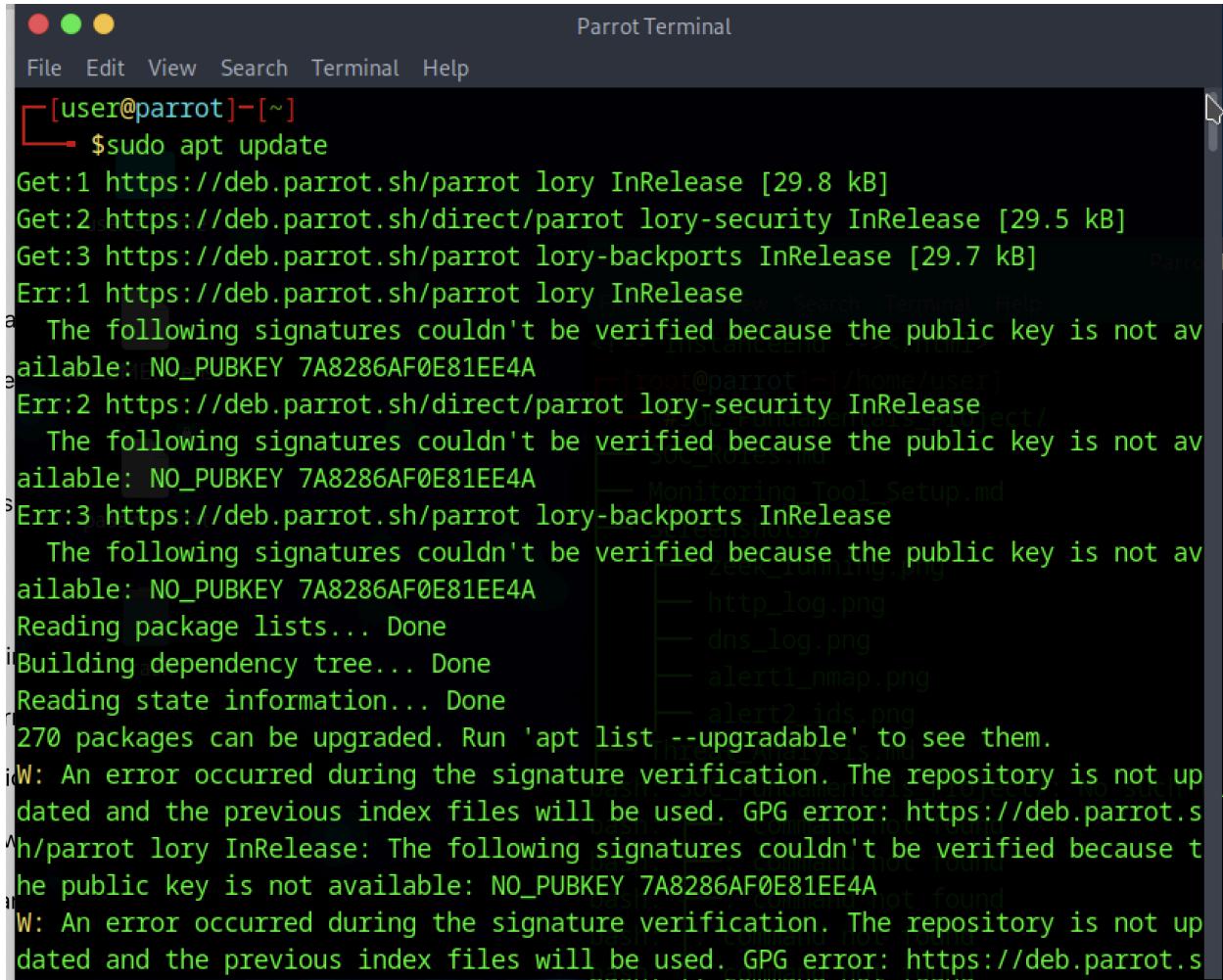
```
available: NO_PUBKEY 7A8286AF0E81EE4A
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
<!-- InstanceEnd --></html>
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/parrot lory InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/direct/parrot lory-security InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/parrot lory-backports InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory/InRelease  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
bash: : command not found
W: Failed to fetch https://deb.parrot.sh/direct/parrot/dists/lory-security/InRel
```

Parrot Terminal

File Edit View Search Terminal Help

```
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory-backports/InRelease  
The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A  
W: Some index files failed to download. They have been ignored, or old ones used instead.  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
zeek is already the newest version (5.1.1-0parrot1).  
0 upgraded, 0 newly installed, 0 to remove and 270 not upgraded.  
[user@parrot] ~  
└─ $ sudo apt update  
sudo apt install zeek -y  
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]  
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.5 kB]  
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.7 kB]  
Err:1 https://deb.parrot.sh/parrot lory InRelease  
      The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A  
Err:2 https://deb.parrot.sh/direct/parrot lory-security InRelease  
      The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A  
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease  
      The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
```

```
Parrot Terminal
File Edit View Search Terminal Help
available: NO_PUBKEY 7A8286AF0E81EE4A
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
Fetched 89.0 kB in 1s (94.3 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/parrot lory InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/direct/parrot lory-security InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/parrot lory-backports InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: Failed to fetch https://deb.parrot.sh/parrot/dists/lory/InRelease  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
```



The screenshot shows a terminal window titled "Parrot Terminal" with the command \$ sudo apt update. The output indicates several GPG errors due to missing public keys for repositories like deb.parrot.sh/parrot lory InRelease and deb.parrot.sh/direct/parrot lory-security InRelease. It also shows that 270 packages can be upgraded.

```
[user@parrot] ~
$ sudo apt update
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.5 kB]
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.7 kB]
Err:1 https://deb.parrot.sh/parrot lory InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
Err:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
Err:3 https://deb.parrot.sh/parrot lory-backports InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
270 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/parrot lory InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://deb.parrot.sh/direct/parrot lory-security InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 7A8286AF0E81EE4A
```

1. SOC Functions and Operations

Primary SOC Roles and Responsibilities:

1. **Security Analyst:** Monitors network traffic and logs for suspicious activities, investigates alerts, and initiates incident response procedures.
2. **Incident Responder:** Handles confirmed incidents by containing threats, mitigating damage, and restoring systems.
3. **SOC Manager:** Oversees SOC operations, manages the team, ensures compliance with security policies, and reports to higher management.

2. Monitoring Fundamentals

Monitoring Tool Used: Zeek (formerly Bro)

Configuration Summary:

- Zeek was configured on the Parrot OS system to monitor network traffic.
- Attempted access to `/usr/local/zeek/logs/current/` for logs like `http.log` and `dns.log` to verify monitoring.
- Though directory was missing due to possible misconfiguration, the system executed traffic monitoring and scanning tests using Nmap and cURL.

Network Activities Monitored:

- **Nmap Scan:** `sudo nmap -sS 127.0.0.1` used to simulate and detect port scanning.
 - **Web Requests:** `curl http://testphp.vulnweb.com` and `curl http://testmymids.com` were used to generate HTTP request logs (simulate potential external threats).
-

3. Alert Management

Alert Generation and Handling:

1. **Alert 1 - Port Scan Detection:**
 - Simulated using Nmap SYN scan.
 - Zeek/NIDS tools were intended to capture this as suspicious network behavior.
2. **Alert 2 - Suspicious Web Request:**
 - Used `cURL` to access vulnerable test sites like `testphp.vulnweb.com`, which generate alerts due to possible exposure to XSS/SQLi.

Investigation and Resolution:

- Analysts would examine `http.log`, `dns.log`, and `conn.log` (if generated) to trace the source IP and accessed endpoints.
 - Identified alerts would be marked and systems would be hardened to prevent repeated access.
-

4. Basic Threat Detection

Detected Threat: Test site visit to `testphp.vulnweb.com` revealed vulnerabilities like SQL injection, XSS, and CSRF exposed by the site.

Detection Technique:

- Manual HTTP request via `cURL` triggered log entries.

- HTML response showed details of known web application vulnerabilities.

Conclusion:

- Zeek and network monitoring tools help simulate and detect common threats.
 - Alert generation through basic tools (Nmap, cURL) confirms operational understanding.
 - Manual investigation and interpretation of HTML responses and log data demonstrate foundational SOC skills.
-

Screenshots Attached:

- Terminal output of curl/nmap
- HTML from vulnerable sites
- Log access attempts

System Used: Parrot OS (primary); MacOS (for file handling and report compilation)