SHODAN for DNS information gathering

(*and the real case of PenTBox*)

Alberto Ortega
alberto[at]pentbox[dot]net
http://pentbox.net/

1.- What is what?

- **DNS information gathering**: Process to find hosts and information using DNS queries. Useful for pentesting (to build a map of the network and find targets).
- **SHODAN**: A computer search engine.
- **PenTBox**: A [security suite | framework] written in Ruby for security, stability and pentesting tasks.

Most of common DNS information gathering techinques are well known and some are quite old (but still working!).

- Common DNS tools:
Fierce
dnsmap
DNSenum
dnswalk
...

2.- The idea

Use SHODAN to find hosts (IPs) inside our targets area and perform reverse DNS petitions (PTR). In addition, SHODAN will bring we useful extra information about the hosts.

DNS → shodan.search(dns_name) → returns → IPs[] → ptr_petitions(IPs[])

3.- Code is fun!!

PenTBox is (one of the first?) programs to implement this technique. The implementation is as follows:

```
#!/usr/bin/env ruby
puts "[*] Searching with SHODAN"
begin
	api = Shodan::WebAPI.new(shodan_api_key)
	query = domain # Something like example.com
	result = api.search(query)
	result['matches'].each do |host|
		print "IP #{host['ip']} #{host['country']} #{host['os']} => "
		result = ptrpetition(host['ip'])
		if result.size == 0
			puts "DNS not found"
		else
			puts result
		end
	end
rescue
	puts "	Error searching with SHODAN"
end
```

The result is something like this:

```
# For apple.com
[...]
IP 17.250.249.** US  => **.249.250.17.in-addr.arpa.   7106   IN   PTR
***b01-photocast.mac.com.
IP 17.251.200.** US  => DNS not found
IP 17.112.171.** US HPUX 10.20 => DNS not found
IP 17.254.20.*** US  => ***.20.254.17.in-addr.arpa.   28707   IN   PTR
***ailme.apple.com.
IP 17.254.20.** US FreeBSD 4.4 => **.20.254.17.in-addr.arpa.   28707
IN   PTR   ***eforipodandiphone.apple.com.
IP 17.251.200.** US  => DNS not found
IP 17.82.254.*** US  => ***.254.82.17.in-addr.arpa.   86307   IN   PTR
***mail.asia.apple.com.
[...]
```

This is only a little sample, but as you can see, we can collect some extra information (country, os) and not only the DNS / IP.

4.- Pros / Cons

Pros

- A new way to find hosts(!).
- Brings more information about the hosts.
- Fast and clean, the infomation is cached in SHODAN, the program only do the PTR petition to an existent IP address.

Cons

- The technique depends of SHODAN.
- In some cases we collect useless or redundant information.

5.- References

http://www.shodanhq.com/
http://pentbox.net/