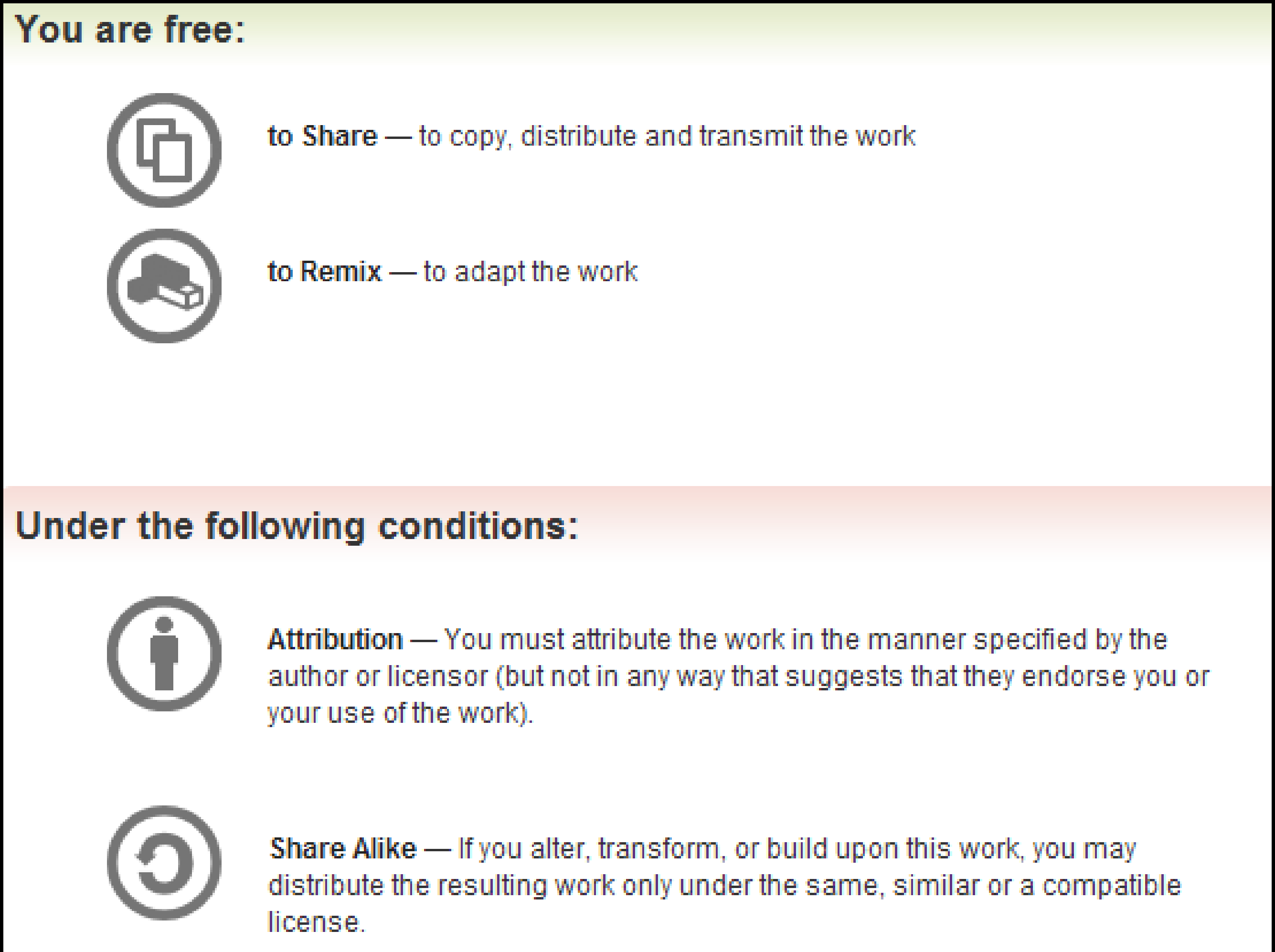
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

# whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

Fingerprinting

Defining what the target really is!

Outline

- External Footprinting
  - Identify External Ranges
  - Passive, and Active
- Internal Footprinting
  - Identify Internal Ranges
  - Passive, and Active

External Footprinting

Identify Customer External Ranges

- The major goals of intelligence gathering during a penetration test is to determine hosts which will be in scope.

- Common techniques to identify:
  - WHOIS searches on the domains and the ranges
  - reverse DNS lookups
  - DNS brute forcing

Passive Reconnaissance - WHOIS Lookups

- Determine TLD for the domain, and which WHOIS server contains the information we're after.
- WHOIS information is based upon a tree hierarchy.
- ICANN (IANA) is the authoritative registry for all of the TLDs.
- Middle East WHOIS lookup (registrar): RIPE NCC, http://www.ripe.net/lir-services/member-support/info/list-of-members/mideast
- DEMO (whois)

Online Tools

- Central Ops, http://centralops.net/
- NetCraft, http://netcraft.com/
- Domain Tools, http://www.domaintools.com/
- DNS Stuff, http://www.dnsstuff.com
- MX Toolbox, http://mxtoolbox.com
- RIPE, http://www.ripe.net/data-tools/db
- WHOIS, http://www.whois.com/whois/
- WHOIS, http://www.whois.sc/
- What Is My IP, http://www.whatismyip.com/
- InterNIC, http://www.internic.net/

Active Footprinting

- **Port Scanning – Next Week**

DNS Discovery

- Performed by looking at the WHOIS records for the domain's authoritative nameserver.

- Variations of the main domain name should be checked, and the website should be checked for references to other domains which could be under the target's control.

Zone Transfers

- DNS zone transfer, also known as AXFR, is a type of DNS transaction.
- It is a mechanism designed to replicate the databases containing the DNS data across a set of DNS servers.
- Zone transfer comes in two flavors, full (AXFR) and incremental (IXFR).
- Tools commonly used: host, dig, and nmap
- DEMO

Forward/Reverse DNS

- Reverse DNS can be used to obtain valid server names in use within an organizational.
- There is a caveat that it must have a PTR (reverse) DNS record for it to resolve a name from a provided IP address.

DNS Bruteforce

- Check the ability to perform zone transfers.
- Discover additional host names that are not commonly known.

SMTP

- SMTP bounce back, also called a Non-Delivery Report/Receipt (NDR), a (failed) Delivery Status Notification (DSN) message, a Non-Delivery Notification (NDN) or simply a bounce, is an automated electronic mail message from a mail system informing the sender of another message about a delivery problem.

- Done by simply creating a bogus address (Blah_blah_address@target.com) within the target's domain.

- DEMO:
  - Central Ops (Email Dossier), http://centralops.net/co/
  - Manually

SMTP – Cont.

smtp-user-enum v1.2 (http://pentestmonkey.net/tools/smtp-user-enum)

- Usage: smtp-user-enum.pl [options] (-u username | -U file-of-usernames) (-t host | -T file-of-targets)

- Examples:
- $ smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1
- $ smtp-user-enum.pl -M EXPN -u admin1 -t 10.0.0.1
- $ smtp-user-enum.pl -M RCPT -U users.txt -T mail-server-ips.txt
- $ smtp-user-enum.pl -M EXPN -D example.com -U users.txt -t 10.0.0.1

Banner Grabbing

- An enumeration technique used to glean information about computer systems on a network and the services running its open ports.
- Banner grabbing is used to identify network the version of applications and operating system that the target host are running.

- Usually performed on: HTTP, FTP, and SMTP
- Tools commonly used: Telnet, Nmap, and Netcat

SNMP Sweeps

- SNMP offer tons of information about a specific system.
- The SNMP protocol is a stateless, datagram oriented protocol.
- Unfortunately SNMP servers don't respond to requests with invalid community strings and the underlying UDP protocol does not reliably report closed UDP ports. This means that "no response" from a probed IP address can mean either of the following:
  - machine unreachable
  - SNMP server not running
  - invalid community string
  - the response datagram has not yet arrived

Web Application Discovery

- Identifying weak web applications can be a particularly fruitful activity during a penetration test. Things to look for include OTS applications that have been misconfigured, OTS application which have plugin functionality (plugins often contain more vulnerable code than the base application), and custom applications. Web application fingerprinters such as WAFP can be used here to great effect.

- **More on this when we reach Web Penetration Testing**

Virtual Host Detection & Enumeration

- Web servers often host multiple "virtual" hosts to consolidate functionality on a single server. If multiple servers point to the same DNS address, they may be hosted on the same server. Tools such as MSN search can be used to map an ip address to a set of virtual hosts.

Establish External Target List

- Once the activities above have been completed, a list of users, emails, domains, applications, hosts and services should be compiled.
  - Mapping versions
  - Identifying patch levels
  - Looking for weak web applications
  - Identify lockout threshold
  - Error Based
  - Identify weak ports for attack
  - Outdated Systems
  - Virtualization platforms vs VMs
  - Storage infrastructure

Internal Footprinting

Passive Footprinting

- If the tester has access to the internal network, packet sniffing can provide a great deal of information.
- Use techniques like those implemented in p0f to identify systems.

```
# p0f –o cap.txt  -i eth0 -M -V -v -p -t
```

Identify Customer Internal Ranges

- When performing internal testing, first enumerate your local subnet, and you can often extrapolate from there to other subnets by modifying the address slightly. Also, a look a the routing table of an internal host can be particularly telling. Below are a number of techniques which can be used.
- DHCP servers can be a potential source of not just local information, but also remote IP range and details of important hosts. Most DHCP servers will provide a local IP gateway address as well as the address of DNS and WINS servers. In Windows based networks, DNS servers tend to be Active Directory domain controllers, and thus targets of interest.

Active Footprinting

We can perform all the external active footprinting techniques here.

Active Footprinting

Port Scanning

- Internal port scanning differs from external port scanning, because of the higher bandwidth available, and the ability
- **Next Week**

Assingment

- Choose a company and gather information about it…

SUMMARY

- We saw what is intelligence gathering
- The OSINT three
- What corporate info to gather
- What individual info to gather
- Understood the covert gathering types
- How to use Google when performing intelligence gathering

References

- Effective meetings, http://www.businessandthegeek.com/?p=112
- http://www.pentest-standard.org/index.php

WHOIS lookup references

- ICANN - http://www.icann.org
- IANA - http://www.iana.com
- NRO - http://www.nro.net
- AFRINIC - http://www.afrinic.net
- APNIC - http://www.apnic.net
- ARIN - http://ws.arin.net
- LACNIC - http://www.lacnic.net
- RIPE - http://www.ripe.net , RIPE NCC