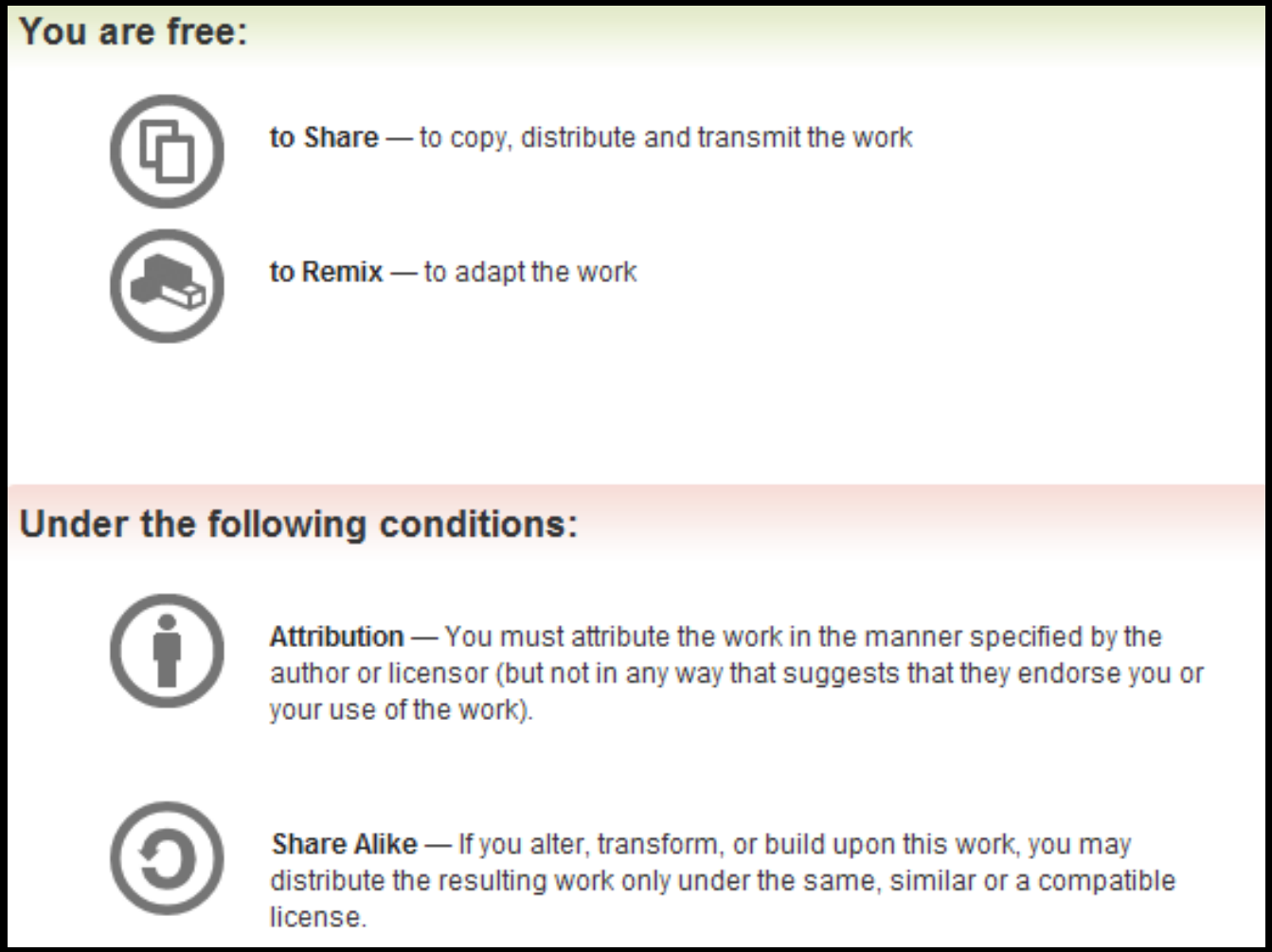
Hacking Techniques & Intrusion Detection

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/



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

Footprinting

Walking the trails to a target

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 Recon - 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)

Passive Recon - NetCraft

- Internet monitoring company that monitors uptimes and provides server operating system detection.
- Site Report returns information such as:
  - IP address
  - Name servers
  - Reverse DNS
  - Netblock owner
  - DNS admin
  - Domain registry
- DEMO

Passive Recon - URL(s)

- Extract list of URLs from a web page
  - list-urls.py
- Search for files in a domain
  - goofile.py
  - FOCA

- DEMO

Online Tools

- Central Ops, http://centralops.net/
- Wayback Machine: http://archive.org/
- Zone-h Defacement Archive, http://zone-h.org/
- 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/

Google for Pentesting

- Check Johnny Long's presentation @Blackhat …
- Google Dorks, http://www.exploit-db.com/google-dorks/
- Google Hacking Database (GHDB), http://www.hackersforcharity.org/ghdb
- Assignment #1: Write about 10 Google Dorks.

ShodanHQ

- ShodanHQ.com is a computer search engine.
- Examining the response of the devices it contacts on the Internet. Information gathered such as:
  - Target OS, Web server software version
  - Checks if default user/pass are being used
  - Can identify webcam, firewalls, and VoIP devices
  - Can identify network printers

- Need Help? www.shodanhq.com/browse
- Registration is required to make the most effective use of the site.

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.

DNS Discovery – DNS Types

- A Host's IP address.
- MX Host/domain's mail exchanger(s)
- NS Host or domain's name server(s)
- CNAME Host's canonical name allowing additional names or aliases

- SOA Authority for the domain
- SRV Service location record often used with Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP)

- RP Responsible person
- PTR Pointer to a canonical name, used for reverse lookups

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

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.

Forward DNS

- Some call it “DNS Bruteforcing”
- Not only zone transfers!
- Discover additional host names that are not commonly known.
  - fierce.pl
  - dnsenum.pl
  - dnsrecon.py

- DEMO

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.

SMTP – Tools

- SMTP User Enumerator, smtp-user-enum
  - smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1
- SMTP Scan, smtpscan
- SMTP Relay Checker, smtprc
- Swiss Army Knife for SMTP, swaks
- Nmap NSE script, smtp-enum-users.nse

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

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.

- **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 Bing 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

- Start by identifying the local subnet, then modify slightly to reach other subnets.
- Check routing tables of hosts.
- Most popular technique used is checking DHCP servers.

Active Footprinting

- We can perform all the external active footprinting techniques here.

Port Scanning:

- Internal port scanning differs from external port scanning, because of the higher bandwidth available, and the ability to get more accurate response.

Next Week

?

- Countermeasure
- Mitigation
- Remediation

Assingment(s)

Assignment #2:

- Gathering information about a website from Google cache, is it an Active or Passive Recon?

Assignment #3:

- Choose a target that you have permission to, maybe yourself and try to gather as much information found publicly as you can. Write a report about that.

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
- What is footprinting
- Difference between active and passive footprinting
- Main external and internal footprinting information resources
- How to use Google when performing intelligence gathering
- Discusses mitigation to footprinting

References

- Effective meetings, http://www.businessandthegeek.com/?p=112
- Penetration Testing Standards, http://www.pentest-standard.org/
- FOCA, http://www.informatica64.com/foca/
- Foundstone,
- Johnny Long, Blackhat, Google Hacking for Penetration Testers,
- Exploit-DB, Google Dorks,
- NetGlub,
- Paterva Maltego,
- 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
- SensePost BiLE Suite, http://www.sensepost.com/labs/tools/misc
- List of DNS Record Types, http://en.wikipedia.org/wiki/List_of_DNS_record_types