Assignment #5, COMP 5370/6270 Instructor: A. Skjellum; TA: A. Ravipati Assigned: October 9, 2015    
Due: October 23, 2015

JCC0044/902521946

Problems 1-4: 25 points each for Ugrads, 20 points each for Grads.

1. Learn & describe what is information foot printing. How does it help crackers vs  hackers.   
   *Note: Definition of cracker and hacker in this context: Cracker – (Black Hat hacker) The intention of cracker is to breach or bypass internet security for malicious gains.*  *Hacker – (White Hat Hacker) The intentions of hacker is to explore vulnerabilities and take measures to patch the vulnerabilities.*

Foot printing is when information about a particular computer, and its related users and systems, is gathered together. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system – not just an email account or a bank account. By finding out everything a system does and has on it, the hacker can become an extremely powerful attacker.

It allows a hacker to get complete access to all your information. A hacker would start with basic information from your website – such as names, email addresses and so on. Next, they can find out the IP address of your website and can check if your server is online – a site like PING will give this information from your web address. A quick Google search will also reveal more information about your site, such as when your domain was registered and when it will expire, networking protocols and so on. A cracker would use this information for malicious gains.

1. Learn about Whois, Nslookup, traceroute? Explain functions of each term.

WhoIs lets you perform a domain whois search, whois IP lookup and search the whois database for relevant information on domain registration and availability. This can help provide insight into a domain's history and additional information. Use WhoIs lookup anytime you want to perform a search to see who owns a domain name, how many pages from a site are listed with Google or even search WhoIs address listings for a website's owner.

Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through Control Panel.

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internal Protocol network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point.

1. What is Nmap?

**Nmap** (*Network Mapper*) is a security scanner originally written by Gordon Lyon (also known by his pseudonym *Fyodor Vaskovich*)used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap is also capable of adapting to network conditions including latency and congestion during a scan. Nmap is under development and refinement by its user community.

Nmap was originally a Linux-only utility,[3] but it was ported to Microsoft Windows, Solaris, HP-UX, BSD variants (includingMac OS X), AmigaOS, and SGI IRIX.[4] Linux is the most popular platform, followed closely by Windows.

1. http://mxtoolbox.com/SuperTool.aspx - Use this tool and write a report.

Steps to make a report using Super tool -

* Consider 3 or more domains (ex: Google, AUBURN.EDU, UA.EDU, Wikipedia.org, one you choose)
* Use Blacklists - Learn about any two blacklists and what they black list, and what it means to black list. What is grey listing?
* Analyze an email header - see DKIM signature. Using online resources to learn what DKIM is and how a DKIM signature helps.
* Goto more> Network > what is my ip . Learn about what information can be extracted if you know an IP address.
* The conclusion of your report should explain what the tool is about. How can it be used in securing any individual domain.

From blacklisting checking Google.com, I found was SORBS (Spam and Open Relay Blocking System), owned and operated by Proofpoint, Inc., provides free access to its DNS-based Block List (DNSBL) to effectively block email from more than 12 million host servers known to disseminate spam, phishing attacks and other forms of malicious email. The list typically includes email servers suspected of sending or relaying spam, servers that have been hacked and hijacked, and those with Trojan infestations. In an attempt to provide preemptive protection, SORBS also lists servers with dynamically allocated IP addresses.

I checked 127.0.0.2 and got blocklist.de. www.blocklist.de is a free and voluntary service provided by a Fraud/Abuse-specialist, whose servers are often attacked on SSH-, Mail-Login-, FTP-, Webserver- and other services.

More information about BLOCKLIST.DE can be found at their website: http://www.blocklist.de/en/index.html

Reason for listing - Infected System, see http://www.blocklist.de/en/view.html?ip=127.0.0.2, Infected System, see http://www.blocklist.de/en/view.html?ip=127.0.0.2

Greylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using greylisting will "temporarily reject" any email from a sender it does not recognize.

DomainKeys Identified Mail (DKIM) lets an organization take responsibility for a message that is in transit.  The organization is a handler of the message, either as its originator or as an intermediary. Their reputation is the basis for evaluating whether to trust the message for further handling, such as delivery. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication.

An IP Address is a way of identifying a computer on a network. Its like a postal address for network data. However There are differnet 'level's of network, Local Area Networks (LAN's) and Wide |Area Networks (WAN's). The computers in a single house would be on a LAN but would connect to an ISP via the modem/cable connection which in turn would connect them to the internet (Which is a WAN).   
  
Depending upon your contract with the ISP you may have a static IP or a dynamic IP. static IP's do not change, you have specifically requested that it doesn't and pay for the privilege. This is usually used by businesses or people hosting their own Web servers. Dynamic IP's are more common and change at the whim of the ISP and can be "leased" for periods as short as an hr.   
  
In most cases an IP address will only lead back to your ISP gateway. Unless the person has inside knowledge of the ISP's IP allocation table (i.e has access to the 'register' of users) that is as far as they will get. The police and other government institutions can get access with a court order but private individuals will not be able to do so. However if what you are doing is illegal then the police could be brought in.

All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool.  Input a domain name or IP Address or Host Name. Links in the results will guide you to other relevant tools and information.  And you'll have a chronological history of your results. These tools pretty much sum up and find issues with an individual domain.

5. Problem Required for Graduate students (extra credit for Ugrad) – 20 points. Study: https://dmarc.org/  See: http://www.mcafee.com/us/resources/solution-briefs/sb-spf-dkim-dmarc- demystified.pdf  Compare and contrast to DMARC, DKIM, SPF.

SPF (Sender Policy Framework) is a DNS text entry which shows a list of servers that should be considered allowed to send mail for a specific domain. Incidentally the fact that SPF is a DNS entry can also considered a way to enforce the fact that the list is authoritative for the domain, since the owners/administrators are the only people allowed to add/change that main domain zone.

DKIM (DomainKeys Identified Mail) should be instead considered a method to verify that the messages' **content** are trustworthy, meaning that they weren't changed from the moment the message left the initial mail server. This additional layer of trustability is achieved by an implementation of the standard public/private key signing process. Once again the owners of the domain add a DNS entry with the **public DKIM key** which will be used by receivers to verify that the message DKIM signature is correct, while on the sender side the server will sign the entitled mail messages with the corresponding private key.

DMARC (Domain-based Message Authentication, Reporting and Conformance) empowers SPF and DKIM by stating a clear policy which should be used about both the aforementioned tools and allows to set an address which can be used to send reports about the mail messages statistics gathered by receivers against the specific domain.

Unfortunately even by having a perfectly functional mail system with all the above tools enforced you won't be 100% safe from the bad guys out there. Not all servers are using all three tools shown above. It's enough to take a look at the table shown in Wikipedia [2] to see how that's possible.

Furthermore there are some limits that you should always consider when dealing with SPF, DKIM and DMARC:

* as already said above DKIM alone doesn't grant in any way that the sender server is allowed to send outgoing mail for the specific domain
* SPF is powerless with messages forged in shared hosting scenario as all the mail will appear as the same coming IP
* DMARC is still in its early age and unfortunately not used as much as hoped to make a huge difference
* DMARC can (and will) break your mail flow if you don't set up **both** SPF and DKIM **before** changing DMARC policy to anything above "none".

6. Extra Credit Problem (Ugrad and Grad) -10 points max.  Study DNS and what it does, and find some attacks against it. Why are attacks on DNS a big danger?  See: https://en.wikipedia.org/wiki/Domain\_Name\_System See: https://en.wikipedia.org/wiki/DNS\_spoofing

Try the Super Tool (see above) to discover properties of DNS (e.g., errors).

The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. The Domain Name System is an essential component of the functionality of most Internet services because it is the Internet's primary directory service.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over sub-domains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.

Types of DNS attacks include:

Zero day attack – the attacker exploits a previously unknown vulnerability in the DNS protocol stack or DNS server software.

Cache poisoning – the attacker corrupts a DSN server by replacing a legitimate IP address in the server’s cache with that of another, rogue address in order to redirect traffic to a malicious website, collect information or initiate another attack. Cache poisoning may also be referred to as DNS poisoning.

Denial of Service – an attack in which a malicious bot sends send more traffic to a targeted IP address than the programmers who planned its data buffers anticipated someone might send. The target becomes unable to resolve legitimate requests.

Distributed Denial of Service - the attacker uses a botnet to generate massive amounts of resolution requests to a targeted IP address.

DNS amplification - the attacker takes advantage of a DNS server that permits recursive lookups and uses recursion to spread his attack to other DNS servers.

Fast-flux DNS – the attacker swaps DNS records in and out with extreme frequency in order redirect DNS requests and avoid detection.

Although the DNS is quite robust, it was designed for usability, not security, and the types of DNS attacks in use today are numerous and quite complex, taking advantage of the communication back and forth between clients and servers. To lessen the chance of a DNS attack, server administrators should use the latest version of DNS software, consistently monitor traffic and configure servers to duplicate, separate and isolate the various DNS functions.