Reaktive Sicherheit

Übungsblatt 2

Balduin Binder [s6babind@uni-bonn.de] Charlotte Mädler [s6chmaed@uni-bonn.de]
Bünyamin Sarikaya [s6busari@uni-bonn.de]

2.2/3.1/4 Fehlen, 2.3 to be translated/written properly

Aufgabe 1

Aufgabe 1.1 Erklären Sie kurz, wodurch Heartbleed ermöglicht wurde.

Das Problem lag bei OpenSSL, eine Applikation die SSL implementiert, nicht mit dem Protokol SSL selbst. OpenSSL wird aber sehr viel benutzt (bei entdeckung von Heartbleed wurde vermutet, dass etwa 50% aller Websiten hiervon betrofffen waren). Server haben nur eine bedingte Anzahl an Sockets, es gibt also ein Timeout für inaktive Verbindungen. Um dies bei aktiver Nutzung zu verhindern schickt der Computer des Nutzers einen sogenannten "Heartbeat" an den Server, um Aktivität zu zeigen. Der Heartbeat kann Daten bis 64kB beinhalten und der Server antworten mit der selben Menge an Daten. OpenSSL überprüft aber nie den Wert der Größe sondern "vertraut" auf dessen Richtigkeit.

Aufgabe 1.2 Erklären Sie kurz, wie Heartbleed für einen Angriff ausgenutzt werden kann.

"Heartbleed" kommt zu stande wenn man bsp. 1kB Daten geschickt hat, dem Server aber gesagt hat es wären z.B. 64kB. Dann schickt der Server den gesendeten 1kB zurück und zusätzliche 63kB die er aus dem Speicher auffüült. Dies könnten unteranderem auch Nutzername/Passwörter/etc. beeinhalten. Ein Angreifer kann diese Daten dann nutzen.

Aufgabe 1.3 Wie können Sie in Ihrer Rolle als Systemadministrator erkennen ob Ihr System von einem Angriff betroffen ist, der durch Heartbleed möglich wurde? Begründen Sie Ihre Antwort.

Ein Heartbleedangriff hinterlässt keine direkten Spuren, also ist es nicht Möglich im Nachhinein konkret zu überprüfen ob Passwörter gestohlen worden sind. Es gibt aber Seiten mit den man testen kann ob es aktuell Verwundbarkeiten gibt (Bsp:http://filippo.io/Heartbleed/ oder das Go-Script Heartbleed) und dadurch eine Gefahr besteht. Zu empfehlen wäre auf OpenSSL 1.0.1G (oder neuer) zu updaten, neue Zertifikate für neu erstellte Keys auszustellen, sie zu installieren und zu verifizieren, die alten zurückzunehmen und sämtliche Nutzernamen und Passwörter (Wichtig, erst danach) zu ändern (Und zwar auf allen eventuell betroffenen Systemen).

Aufgabe 1.4 Ist Heartbleed auch relevant für Clients? Welche OpenSSL-Version verwendeten damals aktuelle Android oder iOS Smartphones? Nennen Sie die von Ihnen verwendeten Quellen.

Applenutzer waren von Heartbleed nicht betroffen. OS X verwendete die ältere OpenSSL-Version 0.9.8, die Heartbleed noch nicht beinhaltete. iOS wiederum kommt standardmäßig überhaupt nicht

mit OpenSSL in Kontakt. Android-Nutzer waren dagegen anfällig, wenn sie Version 4.1.1 (erstes Update von Jelly Bean) installiert hatten. Bei späteren Versionen hat Google dies abgeschaltet. Quelle:https://www.heise.de/mac-and-i/meldung/Heartbleed-Sicherheitsluecke-OS-X-und-iOS-nicht-betroffen-zumindest-nicht-direkt-2167417.html

Aufgabe 2

Aufgabe 2.1 Beschreiben Sie die Vorgehensweise eines Angreifers beim DNS Spoofing

Bei einer DNS Operation gibt der Nutzer eine Website in den Browser ein, der dann den lokalen DNS Server nach der Adresse fragt und dann den User zur gewünschten Website weiter leitet. Hierbei hat der DNS Server einen Cache, wodoruch die Abfrage schneller wird. Wenn die Website nicht im Cache ist, wird der "Master" DNS server via Internet gefragt. Ein Angreifer würde den lokalen DNS Anfragen und wärend dieser auf eine Antwort vom Master DNS wartet, ihn mit gefälschten Antworten überfluten, z.B. alternative Ip-adresse (IP-Spoofing). Diese wird dann in den Cache aufgenommen. Wenn nun ein Nutzer die selbe Anfrage zum lokalen DNS stellt, wird er zur fake-website weitergeleitet (z.b. Phishing oder Pharming) DNS Spoofing wird deshalb auch passend "Cache poisining" gennant.

Aufgabe 2.2 Beschreiben Sie mögliche Schutzmaßnahmen.

Eine mögliche Schutzmaßnahme ist es, das lokale DNS-Chaching zu deaktivieren oder über ein VPN ins Internet zu gehen.

Aufgabe 2.3 Wie konnte es zu den in „The Collateral Damage of Internet Censorship by DNS Injection" beschriebenen Kollateralschäden kommen?

arises from resolvers querying TLD name servers who's transit passes through China rather than effects due to root servers (F, I, J) located in China Collateral damage occurs when a DNS query from a recursive resolver enters a censored network, causing the censorship mechanism to react. Although intuition would suggest that this would be a rare occurrence, there exist several factors which may cause the censor to receive and react to DNS queries from outsiders. Iterative Queries (a simple "lookup" may generate numerous queries, the disruption of any by censorship would cause resolution to fail.), Redundant Servers and Anycast (multiple servers in multiple networks to increase reliability,with 13 different roots and 13 global TLD servers for .com, a resolver may experience collateral damage if a path to any one of these 26 IPs passes into a censored network Anycast:single IP address may represent a widely deployed system of servers.) ,Censored Transit and Dynamic Routing (The paths from the resolver to the authorities is dynamic, routing through a series of Autonomous Systems (AS), If one transit AS implements censorship, then all traffic which passes through that AS experiences censorship, even if both the source and destination are in non-censored networks.)

Aufgabe 3

Aufgabe 3.1 Welche Schutzziele der IT-Sicherheit sind von dem Angriff betroffen?

Aufgabe 3.2 Welche Voraussetzungen muss ein Angreifer erfüllen, um diesen Angriff durchführen zu können?

Er braucht schnell-handelnde Server, relativ in der Nähe des Zielgerätes. NSA: rouge Systeme (FoxACid Servers), spezielle highspeed server (Shooters) die an keypoints des Internets verteilt sind. Quantum Insert attacks benötigen prezise Positionierung und aktionen auf Seiten des Rogue Servers, damit sie den "Wettlauf" gewinnen können, wer zuerst die Seite zum Browser delivern kann. Je näher diese am Ziel sind, je Wahrscheilicher ist es, dass sie gewinnen.

Aufgabe 3.3 Welche Maßnahmen schützen gegen diesen Angriff?

Wenn man die ersten Content-carrying Pakete die zurück kommen als Antwort auf den GET request analysiert, wird eines dieser Pakete die Inhalte für die rogue page beinhalten, wenn ein Angriff vollzogen worden ist (wenn Erfolgreich, dass was als erstes kommt) und das andere wird die legitime Antwort beinhalten. Beide packete werden aber die genau gleiche Sequenznummer haben, also erhält man duplikate TCP pakete mit gleicher Sequenznummer aber unterschiedlichen payloads. Dies kann im Normallfall nicht passieren und man kann als Maßnahme nehmen solch Pakete zu blocken.

Aufgabe 4

Wozu dient das Werkzeug nmap und zu welchem Zwek wurde es entworfen?

Nmap ist ein Netzwerkscanner. Es dient dazu, Netzwerke zu analysieren und Computer in Netzwerken zu analysieren. Unter anderem kann nmap Ports scanne, Betriebssysteme erkennen und Services erkenne, die auf einem Computer laufen.

Geben Sie an, wie man mit nmap ausgewählte TCP- oder UDP-Ports des Hosts scanme.nmap.org scannt. Erklären Sie auch, wie der TCP-Port-Scan funtkioniert.

`nmap domain.com`
Der scan funktioniert so, dass an alle Ports Pakete gesendet werden und analysiert wird welche Ports reagieren bzw. ob Pakete zurück kommen. Anhand dieser Information kann man schlussfolgern ob die Ports offen sind (ein Service hinter ihnen läuft) oder nicht.

Geben Sie an, wie man mit nmap das Betriebssystem des Hosts scanme.nmap.org erkennen kann. Erklären Sie kurz wie diese Erkennung funktioniert.

Mit dem Befehl `nmap -A scanme.nmap.org` lässt sich herausfinden, welches Betriebssystem der Host verwendet.
Nmap benutzt dafür die Erstellung eines Fingerprints, der mit einer Datenbank abgeglichen wir. Es werden bis zu 16 Pakete an bestimmte Ports geschickt und auf den request gelauscht um zu analysieren, welche Services der Hosts am laufen hat und welche Ports offen sind. Aus diesen Informationen wird ein Fingerprint erstellt. Es ist jedoch nie 100% darauf Verlass, dass das von nmap “geratene” Betriebssytem auch wirklich das ist was auf dem Host Rechner läuft.

Geben Sie an, wie man mit nmap die eigene IP-Adresse bei Anfragen spoofen kann.

Mit dem Argument `-S` lässt sich eine Beliebige IP adresse Wählen, die in den Header des Pakets geschrieben wird, den nmap versendet, so dass es für den PC der das paket so aussieht als käme das Paket von dieser Adresse.

Wozu dient das Werkzeug netcat und zu welchem Zweck wurde es entworfen?

Netstat dient dazu, zu analysieren, welche verbindungen von einem lokalen Rechner zu entfernten Rechnern bestehen. Es lässt sich unter anderem die IP der Verbundenen Rechner anzeigen.

Geben Sie an, wie man mit netcat auf einem TCP- oder UDP-Port lauscht.

Mit dem `-l` Parameter kann man netcat sagen, dass es auf den nachfolgenden Port lauschen soll.
`nc -l 3333` würde also auf den port 3333 lauschen.

Wozu dient das Werkzeug netstat?

netstat kann Netzwerkverbindungen, routing tables, interface Statistiken und masquerade connections und multicast memberships anzeigen.

Wozu dient der Befehl sudo netstat -plnt und was beschreibt die Ausgabe dieses Befehls?

`-p` Program: Zeige die PID und das Programm zu jedem Socket
`-l` listening: nur die sockets zeigen die gelauscht werden
`-n` numerisch: Zeige die numerische Adresse anstelle des host, port oder Benutzernamens
`-t` tcp: Zeige Verbindungen

Angenommen Sie betreiben zwei Server im Internet. Server A ist ein Server mit IPv4-Adresse der hinter keiner Firewall steckt. Bei Server B ist ein Server mit IPv4-Adresse. Sie sind sich nicht sicher, ob Ihr Anbieter gewisse Ports durch eine Firewall blockt. Erklären Sie, wie man mithilfe der oben genannten Programme testen kann, welche TCP- und UDP-Ports durch die Firewall des Anbieter von Server B geblockt werden.

Eine Möglichkeit dies zu überprüfen wäre netcat mit folgendem Befehl:

`for i in {1..65535} ; do nc -l $i & done` Hierbei werden einfach alle Ports durchprobiert, und geschaut, ob diese etwas zurücksenden. Diese Methode ist sehr ressourcenlastig.