

A Hacker's Showdown: Playing a real-time novel

Author: Thomas Hackner

Novelle zur Lesung des Beitrags der Hacking Night 2010 in Hagenberg, Oberösterreich, organisiert von der Security/Hacking Group des Hagenberger Kreises. Die Lesung wurde gehalten von Michael Kirchner und in Echtzeit gespielt von Philipp Winter und Thomas Hackner. Lesen auf eigene Gefahr, Eltern haften für Ihre Kinder. Tippfehler sind vorbehalten.

Das 4 mal 6 Meter große Zimmer ist vollgeräumt mit Büchern, alten Zeitschriften und noch älteren CDs, die überall auf dem Boden und dem Schreibtisch verstreut herum liegen. Auf dem Schreibtisch befinden sich noch eine Reihe alter Pizza-Schachteln und einige offene leere Dosen Cola. Neben einer offenen Dose Red Bull steht ein Notebook auf dem sonst schon mit freiem Platz spärlich gesättem Schreibtisch. Dem Notebook sieht man die unzähligen Stunden, die es bereits auf dem Buckel hat, an. Auch an diesem Abend ist es eingeschaltet, jedoch beläuft sich die Nutzung dessen heute einmal auf eine entspanntere Tätigkeit als sonst, dem Spielen des Kommandozeilen-Rollenspiels nethack. Alex, der junge Hacker, der dieses Reich sein Eigen nennen darf, hat sicher schon um die 50 Stunden Spielzeit investiert und ist dem Ende Nahe, als er plötzlich Notiz von einer neuen E-Mail nimmt, die er zuvor schon bekommen hatte. Ein wenig widerwillig, aber dennoch wissend, dass er ja ohnehin nichts Besseres zu tun hat, speichert er den aktuellen Spielstand und startete seinen Mail-Client mutt. Alex liebt es auf der Konsole zu arbeiten. Zum einen arbeitet man hier praktisch mit dem System im Einklang und ist nicht durch die angebotene Funktionalität einer GUI eingeschränkt. Zum anderen ist man auf der Konsole ohnehin viel schneller, als auf einer grafischen Oberfläche, auf der man täglich tausende Kilometer mit der Maus zurücklegen muss, um dann doch nicht direkt beim ersten Mal die richtige Schaltfläche zu treffen. Das Mail stammt von seinem Kumpel D0ra. Er pflegt regen Kontakt mit ihm und ist einer der wenigen Leute, denen er vertraut. Vertrauen ist in dem Business ohnehin ein sehr wertvolles Gut und sollte wenn überhaupt nur sehr ausgewählten Leuten geschenkt werden.

"Hi ehkeh, wirf doch mal einen Blick in chan."

Die Mail war kurz und bündig, aber das ist Alex ja gewohnt. Er startet seinen IRC-Client irssi und verbindet sich mit dem IRC-Server, den die Crew nutzt, um Kontakt zu halten. Die Crew besteht aus ein paar Jungs, die sich nun schon länger kennen und ab und an Daten und Informationen über neueste Exploits, Techniken oder Aufträge austauschen. Anscheinend dürfte D0ra wieder etwas gefunden, denn sonst wartet er meist, bis man sich zufällig im IRC trifft. Ja, da war er auch - D0ra erwartet Alex bereits im Channel.

D0ra> Sup?

ehkeh> nix, war grad am zocken, was gibts?

D0ra> du glaubst nicht, was mir gestern passiert ist...
ehkeh> sag schon, wenns nix interessantes is, geh ich lieber zocken
D0ra> ne, bleib noch da - ich war ja heute in barca - war übrigens ein echt cooler trip
D0ra> fescche katzen, unmengen an bier und ach was... ich machs kurz
D0ra> ich hab heute am weg vom flughafen nach haus im taxi ein iPhone gefunden
D0ra> ich wollte es ja schon dem taxifahrer geben, als ich gesehen hab, dass das ding eine prägung auf der seite hatte
D0ra> wer lässt sich denn sein iPhone prägen? naja, whatever, auf jeden fall dachte ich, dass es vl jemanden interessanten gehören könne, jetzt hab ichs mitgenommen und dir übrigens auch schon vorbei gebracht
D0ra> liegt in deinem postkasten, du penner hast ja wieder mal nicht aufgemacht, als ich dort war
ehkeh> ja, kann schon sein, hab gepennt
ehkeh> und was soll ich jetzt mit dem ding?
D0ra> ja siehs dir mal an, vl is was interessanteres drauf; wenn nicht, geben wirs wieder zurück und kassieren finderlohn
D0ra> ich hättts ja selbst versucht, aber die dinger sind ja mit 256 bit AES verschlüsselt
ehkeh> jaja, ich sehs mir mal an, hab ja ohnehin nix bessers zu tun
D0ra> n1, dann meld dich ,wenn du was weißt, dann schau ich mit einem bier vorbei
ehkeh> geht klar, cya
D0ra> cya

Ein wenig müde noch vom Nichts-Tun - das ist oft anstrengender, als man denkt - steht Alex vom Sessel auf und macht sich auf dem Weg zum Postkasten. Die Abendsonne brennt in den Augen, als er die Tür nach außen aufstößt. In langsamen Schritten nähert er sich dem Postkasten und da war es auch, ein kleines Paket ohne Absender, das konnte wohl nur von seinem Kumpel stammen. Zurück im Zimmer packt er das iPhone aus und legt es neben seinem Notebook auf den Tisch. Da war doch kürzlich erst was mit iPhone und Ubuntu, oder? Nach kurzem Überlegen fiel es ihm wieder ein, irgend eine Race-Condition war doch Schuld daran, dass man das Dateisystem mounten konnte, ohne, dass man das Passwort zur Entschlüsselung eingeben musste. Funktionierte allerdings nur bei iPhones, die vor dem Abschalten nicht gesperrt wurden, aber stand das Glück heute ja auf seiner Seite. Alex steckt das iPhone an seinen PC an und startet es. Schon meldet das Betriebssystem eine gemountete Partition, das konnte nur das iPhone sein. Ein Blick in den entsprechenden Ordner bestätigt dies nur. "Sehr gut, fängt ja schon mal gut an", dachte sich Alex, als er sich daran macht das Smartphone nach interessanten Daten zu durchsuchen. Es dauert nicht lange, bis er auf ein sehr interessantes Foto stieß. Alex hält kurz inne, hat er wirklich so viel Glück auf einmal? Ein Blick in die Datei verrät, dass es sich wirklich um Zugangsdaten handelt könnte: "Benutzer: jrock, Passwort: ab!zzy.43444, Domäne: paroit". Spätestens jetzt ist die Neugier von Alex vollständig geweckt. Er hatte Zugangsdaten auf einem iPhone zu irgend etwas gefunden, das sich wohl „paroit“ nennt. Mal sehen, was hier wohl dahinter steckt.

Bevor er jedoch seine erste Amtshandlung antritt, muss noch für genügend

Anonymität gesorgt werden, um nicht bei irgend etwas erwischt zu werden. Zu diesem Zweck startet Alex Tor. Tor ist schon ein nützliches Tool, wenn es um die Verschleierung der Identität im Internet dreht. Das Onion Routing Protokoll versendet alle Daten über mehrere im Netzwerk teilnehmende Server ohne die Identität der Source zu speichern. So kann man unerkannt im Internet surfen, jedoch mit dem Nachteil, dass es immer ewig dauerte, bis die Pakete durch das Netzwerk geschleust werden. Dies ist jedoch der Preis, den man wohl für ein wenig Anonymität zahlen muss. Um zu testen, ob er auch wirklich Tor benutzt, besucht Alex die Seite „check.torproject.org“, die ihm anzeigt, ob sein Browser nun auch wirklich das Tor-Netzwerk zum Surfen verwendet. Den ersten Versuch würde Alex mit der Webseite versuchen und so tippt er einfach blindlinks "paroit.org" in die Titelleiste ein. Und tatsächlich erscheint auf dem Bildschirm eine Webseite einer Firma. Nach ein wenig herum stöbern auf der Seite findet er unter Kontakt den Namen John Rock wieder - der passte doch wunderbar zu dem gefundenen Benutzernamen. Alex ist also auf der richtigen Spur, aber was machte die Firma überhaupt? Anscheinend handelt es sich um eine sehr kleine Firma, die jedoch, wie es den Anschein hat, mit Forschung eine goldene Nase verdient. Interessant genug, um einen etwas genaueren Blick auf sie zu werfen.

Im Grunde fängt jetzt eine Standardprozedur an, die Alex schon oft genug durchexerziert hatte, um sie bereits fast automatisiert ablaufen zu lassen. In der ersten Phase werden Informationen über das Ziel gesammelt. Die Untersuchung der Webseite hatte er im Bezug auf Informationen schon hinter sich gebracht. Nun folgt das Sammeln von Infos über die Domäne des Servers. Mit dem Kommandozeilentool "whois" gelangt er an die Daten des Domäneninhabers und weitere IP-Adressen der Firma. Im nächsten Schritt lokalisiert Alex den Standort es Servers, um einen Eindruck davon zu bekommen, wo er denn überhaupt arbeitet – ist ja nicht immer so klar im Zeitalter des Internets. Nach den initialen Schritten der passiven Informationsbeschaffung muss er ein wenig offensiver werden. Mit nmap, dem Network Mapper, startet er einen Portscan, um auf verfügbaren Dienste des Servers zu testen, und siehe da, er wird auch fündig. Der Server besitzt einen Webserver auf Port 80, den Alex ja bereits kannte. Weiters findet er den SSH-Port 22 und Port 21 für FTP offen vor. Interessanterweise sind noch eine Vielzahl weiterer Services installiert. Wie es aussieht, läuft ebenfalls ein distcc-Dienst und Tomcat auf dem Server der Firma.

Zuerst versucht er einmal das Offensichtlichste: die sogenannten "low hanging fruits". Er nimmt seine gefundene Benutzername-Passwort Kombination und versuchte sich am SSH-Port einzuloggen, doch leider sind die gefundenen Daten wohl für ein anderes System bestimmt. "Wird wohl doch etwas schwieriger", denkt sich Alex und macht sich an die Schnittstelle, die aus Erfahrung die meisten Fehler beherbergt - dem Webserver. Mit "telnet" verbindet sich Alex zum Server, und tippt eine falsche URL ein, um die Antwort des Servers abzuwarten und weitere Informationen zu sammeln. Wie es aussieht, handelte es sich um einen aktuellen Apache-Webserver, von dem er jetzt nicht auswendig Schwachstellen kennt. Also entscheidet sich Alex weiter zu suchen. Nachdem er die Seite ja schon prinzipiell

abgegrast hatte, versucht er ein paar der gängigsten URLs, hinter denen sich oft interessante Informationen versteckt, wie: /intranet, /private, /secret, /intern und da war es auch schon. Klar, soll ja auch leicht für die Mitarbeiter zu merken sein. Alex sitzt einer Anmeldemaske gegenüber, die ihn wahrscheinlich vom Zugang zum internen Bereich abhält. Auch hier versucht er ein paar Standardkombinationen, wie "admin : admin", "admin : [blank]" oder auch seine neu erworbene Benutzername-Passwort Kombination. Aber auch hier kann er sich nicht einloggen. Zumindest einen Benutzernamen hat er ja. Wäre ja sonst wohl auch zu einfach gewesen. Oft haben Firmen zur Anmeldung eine SQL-Datenbank dahinter, um die Benutzer besser verwalten zu können - mal sehen, was sich hier machen lässt. Alex versucht nun einmal "jrock" im Benutzerfeld und ein Hochkomma im Passwortfeld. Eingeloggt ist er nicht, aber irgendwie wurde die Anfrage auch nicht richtig verarbeitet. Toll, denkt sich Alex, dürfte wohl wirklich auf SQL-Injections anfällig sein. Also, im nächsten Schritt - gleich mal den Klassiker ausprobieren ' or '1'='1'. Meist sind SQL-Befehlen bei Logins in der Form `SELECT * from users where username='$username' and password='$password'` aufgebaut. Die Eingabe von Alex würde bewerkstelligen, dass der Aufbau des Kommandos umgebaut würde auf `SELECT * from users where username='jrock' and password=' or '1'='1'`. Das heißt, die Abfrage würde in jedem Fall, auch wenn das Passwort nicht stimmen würde, ein richtiges Ergebnis liefern, und das tat es. Alex grinst in sich hinein – ist ja doch nicht so schwer. Doch beim Durchsuchen der Seite wird sein neu entstandener Übermut sofort wieder auf den Boden der Realität geholt. Leider ist nichts interessantes zu finden. Anstatt brisanten Daten findet er nur eine alte ungewartete Seite wieder, die ihn keinen Schritt vorwärts bringt.

Also nochmal von vorne, was gibt es denn noch Interessantes auf dem Server. Alex entschließt sich dazu sämtliche interessante Kombinationen für URLs durch zu probieren, um vielleicht doch noch auf ein geheimes Verzeichnis zu stoßen und startet zu diesem Zweck Burp. Er lädt eine vorbereitete Liste mit möglichen Verzeichnisnamen in das Programm und startet den Suchdurchlauf. Während dieses Tool nun alle Kombinationen durchprobiert, hat er Zeit sich die anderen Services ein wenig näher anzusehen. Er könnte den SSH-Dienst Bruteforcen, also jede Benutzername-Passwort Möglichkeit durchprobieren, aber das wird wohl der letzte Ausweg, schließlich dauert dies meist ein wenig und verursacht ganz schön viel Lärm. So beschließt er mit dem Tomcat weiter zu machen. Alex startet sein Lieblings-Exploit-Toolkit Metasploit. Schon eine coole Sache, wenn man die meisten Werkzeuge mitsamt Exploits und Scripts in einem Tool vereint herunter laden kann und noch dazu gratis. Alex durchsucht die Exploitsammlung von Metasploit nach etwas Passendem. Er entscheidet sich zuerst für den Login-Scanner, der gängige Username-Passwort Kombinationen durchprobiert. Dazu wählt er den Exploit aus und setzt die entsprechende Ziel-IP und -Port. Anschließend wird mit „exploit“ der Scanner gestartet. Da! Da, war was! Haben die doch tatsächlich den Standardbenutzer tomcat noch installiert! Alex rückt seinen Sessel zurecht – jetzt wird es wieder spannend! Im nächsten Schritt wählt er den Exploit zum Deployen von WAR-Archiven über die Admin-Oberfläche von Tomcat aus. Dazu benötigt er nun auch die vorhin gefundene Benutzername-Passwort-Kombination. Als Payload, also der Code, der auf dem Zielrechner ausgeführt werden würde, wenn der Angriff

erfolgreich verläuft, wählt er eine Back-Connect-Shell, also ein Script, das sich vom Zielrechner zurück zum eigenen Rechner verbindet. Braucht zwar mehr Platz im Speicher, als eine normale `"/bin/sh"` bind-Shell, aber ist zuverlässiger für den Fall, dass eine Firewall dazwischen die direkte Kommunikation auf einen neuen Port verbietet. Anschließend wählt Alex noch einmal den herausgesuchten Exploit aus und tippte das Kommando `"exploit"` in die Konsole, um den Angriff zu starten. Sieht gut aus, warten, und bingo! got a shell! Dies war einer der Momente, für die Alex lebte, keine 15 Minuten und schon ist man wieder Herr eines Netzwerkes einer Firma, die sich irgendwo auf dieser Welt in Sicherheit wälzt und nicht daran denkt, dass es ein Akt von ein paar Minuten wäre, ihre Existenz zu zerstören. Mal sehen was sich hier nun so alles anstellen ließe. Nach ein paar Blicken das `/home` und `/var/www/` Verzeichnis, muss sich Alex jedoch eingestehen noch nicht ganz Herr des Netzwerkes zu sein. Zum einen fehlen ihm noch die Dokumente, die er hätte seinem Freund D0ra stolz präsentieren können, und zum anderen findet er in der Datei `/etc/hosts` noch einen anderen eingetragenen Rechner im Netzwerk.

Alex überlegt noch kurz, ob er nicht nmap herunter laden sollte, es im `/tmp` Verzeichnis extrahieren und den nächsten Scan durchführen sollten. Um Zeit zu sparen, versucht er jedoch einfach per Hand, ob er offene Standardports, wie 21, 23 ..od...ah....der Telnet Port scheint doch offen zu sein. Solche Ports findet man normalerweise nur mehr bei alten Druckern, Switches oder Routern wieder. Er versucht es ein letztes Mal mit seinem Account, den er vom iPhone gestohlen hatte und dieses Mal klappt es. Er hat Zugang zum System erlangt - yeah! Schnell wurde ihm klar, dass es sich wohl nicht um ein Netzwerk-Infrastruktur-Gerät handeln dürfte, sondern um ein Gebäudesteuerungssystem. Das ist einmal etwas anders und eigentlich noch dazu ganz schön cool. So kann er vielleicht sogar Zugangskontrollen außer Kraft setzen, Räume überwachen oder abhören, oder sich auch einfach ein wenig damit herum spielen. Nachdem ohnehin niemand in der Firma sein dürfte, entschließt er sich, ein paar einfache Kommandos auszuprobieren.

Kapitel 2

Wenn er nicht ohnehin schon vorher über SMS alarmiert worden wäre, wären ihm wohl die plötzlichen Lichtwechsel im Haus aufgefallen, die sich hier um 2 Uhr in der Früh im Gebäude der Paro-IT Forschungseinrichtung ereignen. Emil ist Angestellter der Security Enforcing GmbH und hat an diesem Abend Nachtdienst im Security Operations Center. Die Firma, in der er arbeitet, ist darauf spezialisiert Angriffe auf die Netzwerke ihrer Kunden zu erkennen und entsprechend präventive Maßnahmen zu treffen. Zudem ist es Teil seines Jobs anschließend die Polizei zu informieren. Letzteres brachte aber in dem meisten Fällen ohnehin nicht viel, bis die Verfahren endlich ins Laufen kommen, hatten die meisten die Spuren so gut verwischt, dass es ohnehin sinnlos war weiter nach ihnen zu suchen. Emil, ein Mitte 20 Jahre alter Computerfreak mit langen brünetten Haaren, hat schon mehr Erfahrung, als man seinem Alter zumessen würde. Seine Laufbahn als findiger Hacker begann schon mit 8, als er seinen ersten PC von seinem Vater geschenkt bekam. Nach langer Zeit auf der Seite der Angreifer, wechselte er schlussendlich vor 5 Jahren auf die andere Seite und setzte sein Wissen nun zum Schutz von Firmen ein, wenngleich er seine

Vergangenheit dennoch nicht vergessen konnte und auch nicht wollte. Das rote Licht auf einem seiner Operator Bildschirme reißt Emil aus einem seiner Tag/Nachtträume. "Paro-IT, Paro-IT, das is doch diese kleine Forschungsfirma. Nun gut, mal sehen was dort los ist. Wird wahrscheinlich einer dieser zahlreichen Fehlalarme sein. Die sollten echt mal die IDS besser einstellen, Fehlalarme werden auf Dauer ganz schön nervig."

Emil hat einen SSH-Zugang zum Server der Firma Paro-IT und verbindet sich zum Server, um die Situation einmal genauer unter die Lupe zu nehmen. In den Logs heißt es ja, dass ungewöhnlich viel HTTP-Traffic auf dem Webserver war. Ein Blick in die Apache-Webserver-Logs bestätigt dies. Anscheinend ist gerade jemand daran den Webserver auf alle möglichen interessanten Verzeichnisse zu testen. "Sieht schon mehr nach einer gezielten Attacke aus, als sonst", überlegt sich Emil, während er sich langsam aus seinem gemütlichen Sessel aufsetzt. "Solange er nur scannt, ist es noch nicht so schlimm." Emil tippt die IP aus den Logs in eine whois-Abfrage ein. Sieht irgendwie eigenartig aus, wahrscheinlich einer dieser Mächtegern-Hacker, die des Nachts über Tor ihre Script-Kiddie-Tools anheizen. Bisher konnte Emil nicht erkennen, dass ein Einbruch stattgefunden hätte, aber er würde Mal ein Auge darauf behalten und so sucht er weiter. Beim Ausführen des Befehls "who" jedoch bleibt kurz sein Atem stehen. Dürfte es dieser kleine Mächtegern-Kiddie es wirklich geschafft haben, sich auf dem Server einzuloggen? Scheiße, jetzt heißt es schnell handeln. Für die Übergabe der Infos an die Polizei würde er jedoch mehr benötigen, als bloß die IP eines Rechners, der wahrscheinlich nur der letzte in einer Reihe von Rechnern zur Verschleierung der Identität ist. Kurzerhand beschließt Emil die richtige IP heraus zu finden, um auch rechtlich weiter vorgehen zu können. Aus einem seiner vielen Ordner kramt er ein Text-File mit einem HTML-Code-Snippet heraus, das er früher gerne dazu verwendete, um die richtige IP von Freunden zu demaskieren, wenn er sie ärgern wollte. Emil fügt den Code auf der Titelseite der Homepage ein. Jetzt heißt es warten, bis der Angreifer den Köder aufspürt und reagiert. Das Code-Stück bindet ein I-Frame von der Seite decloak.net ein, welche auf verschiedene Arten versucht an die wirkliche IP des Besuchers zu kommen. Unter anderem werden Java-Applets direkt im Browser des Clients ausgeführt und sind diese signiert, lassen sich so auch neue Verbindungen aufbauen bzw. Wege finden, um an die richtige IP-Adresse des Hosts zu kommen. Als Emil noch gerade am Überlegen ist, woher dieser Angriff denn kommen könnte, hat er auch schon eine Antwort. Der Angreifer besuchte anscheinend gerade eben die Index-Seite und so kann Emil die Adresse über die Seite decloak.net auslesen.

Eigentlich wäre das Spiel hier für Emil vorbei. Den Angreifer kicken, den Server abdichten und die Administratoren informieren - so steht es im Handbuch. Doch was würde es bringen einen Angreifer an die heimische Polizei zu übergeben, wenn der inzwischen seine Spuren verwischt? Bis hier alle Verbindungen zu Behörden hergestellt wären, wäre der Angreifer schon wieder längst über alle Berge. Nichts da, da hat er sich mit dem falschen angelegt. Wenn der Angreifer wohl so heiß auf Dokumente ist, sollt er sie auch haben. Emil sucht sich ein beliebiges öffentliches PDF, startet Metasploit und infiziert das PDF mit entsprechendem Schadcode. Eine Backconnect-Shell wählte er aus, für den Fall, dass sich der Angreifer hinter einer

Firewall befindet. Im nächsten Schritt lädt er das PDF auf den Webserver hoch und benennt es in "RD_latest.pdf" um, um es dem Angreifer wieder schmackhaft zu machen. Emil muss nicht lange warten und schon darf er in Metasploit einen Verbindungseingang verzeichnen - Hell Yeah! So macht der Job doch schon wieder Spaß. Emil hat Zugang zum Notebook des Angreifers und noch dazu mit entsprechend guten Rechten. "Das wars nun wohl für dich", denkt sich Emil, als er die zerstörenden Buchstaben "rm -Rf /" in die Konsole eintippt, die Verbindung schließt, den Angreifer aus dem Server von Paro-IT kickt und anschließend zum Telefon greift, um die Systemadministratoren vom Angriff auf ihr Netzwerk zu informieren. Ein Lächeln macht sich auf dem weißen Gesicht des Computerspezialisten breit, nachdem er das Telefonat beendet, sich gemütlich in seinen Stuhl zurück lehnt und langsam in der Nostalgie seiner früheren Zeiten versinkt.

Dieses Werk ist unter einem Creative Commons Namensnennung 3.0 Unported Lizenzvertrag lizenziert. Um die Lizenz anzusehen, gehen Sie bitte zu <http://creativecommons.org/licenses/by/3.0/> oder schicken Sie einen Brief an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.