Table of Contents

Vorwort

Dies ist die erste Fassung des Dokumentes mit einem publizierten Stand vom 23.05.2025. Dieses Dokument diente mir persönlich zur autodidaktischen Fortbildung zu dem Thema Security und Forensik. Dieses Werk ist eine Sammlung an Notizen die in ein Schriftwerk umgeschrieben worden.

Forensik

Es gibt zwar keine einheitliche Definition von IT-Forensik, aber gemeinhin geht es dabei um die methodische Analyse von Daten auf Datenträgern und Computernetzen, um Vorfälle aufzuklären. Die Forensik kümmert sich also darum, dass der Angriff auf ein System aufgeklärt wird. Dafür werden Informationen gesammelt und Berichte erstellt.

Für die Sicherheit und Härtung von Netzen und Systemen ist ein separates Security-Team zuständig. Das Team gibt die Vorgaben für die Ciphers, die Software, die eingesetzt werden darf und die Konfiguration der Netze und Systeme.

Die beiden Gruppen von Administrator*innen nutzen also die gleichen Werkzeuge, Dateien und Konfigurationen. Ein Team sorgt dafür, dass es zu keinem Einbruch kommt, während das andere Team die Sachlage nach einem erfolgreichen Angriff auswertet.

Was Tun Wenn Es Zu Spät ist

Hier findest du einen Leitfaden zum Thema digitale Forensik. Der Fokus liegt dabei vor allem darauf, was zu tun ist, wenn ein System kompromittiert wurde. Es werden Werkzeuge erwähnt, deren Einsatzzweck erklärt und vereinfachte Beispiele hierzu gezeigt. Hier geht's nicht um ein Tutorial, ein How To oder eine genaue Vorgehensweise. Das ist jetzt nicht das Ziel dieses Schriftwerks und die Fälle sind zu individuell, um da eine genaue Vorgehensweise festzulegen. Für jede Situation sollte somit dieser Leitfaden als Stütze, als Unterstützung und als Nachschlagewerk dienen.

Auch wird in diesem Leitfanden eine kurze Vorgehensweise beschrieben, mit Handlungsanweisung bei der Kommunikation mit Angreifern, welche Schritte beachtet werden sollen, die technische Umsetzung für eine Analyse des Angriffes und wie mit Kunden und Beteiligten kommuniziert werden soll.

Für die Analyse und die Arbeiten brauchst du technische Vorkenntnisse und musst die betroffenen Systeme verstehen.

Vorgehen bei Angriffen

Was dann?

Wenn ein System kompromittiert wurde und die Firma oder das Team nicht weiß, wie man eine forensische Arbeit macht, sollte man die Aufgabe lieber an externe Dienstleiter weitergeben. Es

kann auch Sinn machen, das an externe Leute zu übergeben, dass die Administrator*innen befangen sein könnten und eine Überprüfung damit nicht unabhängig durchgeführt werden kann.

Bei Kunden und deren Systemen soll eine überlegte Kommunikation stattfinden.

Welche Informationen sollen geteilt werden?

Weil wir nicht wissen können, was genau passiert ist, sollten wir in der Kommunikation darauf achten, dass wir keine Fakten schaffen. Das könnte den Kunden verunsichern und auch zu widersprüchlichen Aussagen führen. Man kann zum Beispiel nicht davon ausgehen, dass keine Daten abflossen. Hier muss man sagen, dass die Wahrscheinlichkeit, dass Daten abfloßen, ziemlich gering ist.

Angriffsarten

Es gibt verschiedene Gründe und Szenarien für einen Angriff. Entweder ist es ein gezielter Angriff. Dabei wird das System vorher analysiert, beobachtet und dann mit individuellen oder gezielten Angriffen attackiert.

Auch nicht bekannte Sicherheitslücken können ausgenutzt werden oder es findet Social Engineering statt. Die Angreifer können sich dann über Mail oder Telefon Zugang zum System verschaffen.

Schwachstelle Mensch

Ein gezielter Angriff ohne die Ausnutzung von technischen Sicherheitslücken könnte zum Beispiel so aussehen:

Der Angreifer schickt den Mitarbeitern des Unternehmens eine Phishing-Mail. Damit kann er sich zum Beispiel Zugang zu deren Accounts verschaffen. Es besteht die Möglichkeit, dass der Angreifer E-Mails versenden kann. Dadurch könnte er sich als Mitarbeiter ausgeben und über ein Ticket an den Dienstleister eine Nachricht schicken, um einen Public Key zu hinterlegen.

Dadurch könnte der Angreifer ohne technische Lücke Zugriff auf das System bekommen und eine Hintertür einrichten.

Schwachstelle Technik

Es gibt noch eine andere Option, und zwar den Angriff durch Ausnutzen einer Sicherheitslücke. Dann könnte eine

manipulierte Datei einspielt werden. Dadurch würde sich eine temporäre Root Shell öffnet.

Angriffe können durch das Grundrauschen im Internet durchgeführt werden. Das Grundrauschen sind durchgehende Scans gegen die 4.294.967.296 möglichen IPv4-Adressen und offenen Ports. Es wird auch automatisch gecheckt, ob sich hinter dem Port die erwartete Anwendung befindet. Mit Header-Checks wird nach möglichen Versionen gesucht, die für Sicherheitslücken anfällig sind. Oder ob sich hinter der IP-Adresse und dem Port eine ungeschützte Anwendung befindet.

Bei einem Fund einer Softwareversion der Anwendung, die von dem Tooling angegriffen werden kann, dann wird dort entweder Schadsoftware ausgerollt oder es kommt zu einem Datenabfluss.

Ramsonwar As A Service

Das klassische Bild vom Hacker, der gezielt Systeme angreift, um sich selbst zu bereichern, ist hier nicht mehr aktuell. Diese Hacker haben kriminelle Unternehmen gegründet, in denen verschiedene Mitarbeiter*innen arbeiten.

Die Profiteure machen sich selbst nicht mehr die Hände schmutzig, sondern lassen das von anderen machen. Dabei werden kleine Administratoren, Entwickler und Hacker*innen in prekären Lagen rekrutiert. Die RaaS Unternehmen arbeiten tatsächlich mit Headhuntern zusammen und vermitteln zwischen den ausführenden Personen.

Wenn Kryptotrojaner zum Einsatz kommen, kennen die Angreifer den Entschlüsselungskey nicht. Den müssen sie erst erfragen. Die RaaS-Hackbutzen haben auch Supporter, die den Angegriffenen helfen, Geld über BitCoin oder andere spekulative Hashwerte zu überweisen. Auch RaaS Hackbutzen wissen, dass sie schneller und garantierter an ihr Geld gelangen, wenn sie dem Kunden helfen. Kunden, die mit dem Service zufrieden sind, sind eher bereit, zu bezahlen, als zu warten oder sich mit der Materie zu beschäftigen.

Die IT-Leute, die für die RaaS-Hackbutze arbeiten, haben oft keine Ahnung, was genau da eigentlich warten und supporten. Aus alten Resten wurden Maschinen zusammengeschraubt und Administratoren damit beauftragt, Kundenserver zu verwalten. Dabei ist es sogar passiert, dass die Admins nicht wussten, dass sie sich auf einem Command And Control Server befinden. Wenn der Administrator hochgenommen wurde, kann er die anderen höheren Positionen im Unternehmen nicht anschwärzen, weil die Hierarchie unbekannt ist. Die Profitüre

arbeitet in einem klassischen Pyramidensystem oder vermietet ihre Anwendungen, so wie es bei einem Franchiseunternehmen üblich ist.

Die Angreifer sind dann meistens Bauernopfer oder Scriptkiddies für staatliche Akteure oder Kriminelle banden, die bei Hackbutzen die Tools einkaufen oder für diese arbeiten.

Infrastruktur von Erpresser

Die Technik und Infrastruktur, die Agreifer nutzen, wird manchmal mit Teilen vom Flohmarkt zusammengestellt, weil man dafür keine besondere Technik braucht.

Die Server stehen dabei meistens in Ländern, in denen es weniger strenge Regeln gibt, oder wurden von jemand gehackt.

Der Verlust der Hardware soll für die Angreifer nicht schmerzhaft und ersetzbar sein.

Wenn Rechenkapazitäten benötigt werden, wird diese separat angemietet. Zum Beispiel, um gehashte Passwörter aufzubrechen. Hierfür werden leistungsstarke Grafikkarten benötigt. Entweder stehen diese Recheneinheiten abseits der Infrastruktur, damit bei einem Auffliegen nicht auch die teuren GPUs verloren gehen, oder es wird sich Rechenleistung im Internet geklickt, wenn nicht Server mit starken GPUs bereits gekapert wurden.

Verhandeln mit Erpressern

Angriffe haben immer mehrere Ziele, die verfolgt werden. Einerseits kann der simple Schaden eines der gewollten Ziele sein, andererseits kann es auch die Übernahme eines Systems geben, um dieses als Botnetz oder zum Minen zu benutzen.

Eines der wirtschaftlichen Ziele ist es, durch den verursachten Schaden an Geld oder Informationen zu kommen. Bei der Wirtschaftsspionage wird versucht ein Datenabfluss zu verursachen und somit an Informationen eines Unternehmens zu gelangen, ohne bemerkt zu werden.

Erpresser hingegen verfolgen ein direkt monetäres Ziel. Sie möchten mit dem Angriff an Geld gelangen. Entweder durch die Verschlüsselung der Daten und damit durch den Ausfall und wirtschaftlichen Schaden Druck aufzubauen oder durch die Drohung der Herausgabe der Daten an die Konkurrenz Ängste zu schüren.

Wie kommuniziert eins mit Erpressern

Wenn ein Backupkonzept besteht, aus welchen das System schnell wiederhergestellt und der reguläre Betrieb wieder aufgenommen werden kann, ist es nicht nötig auf die Forderungen von Erpressern einzugehen.

Die Hackbutzen lassen immer den Level 1 Support arbeiten, damit die CEOs der RaaS Unternehmen verdeckt bleiben.

Wenn du mit den Erpressern kommunizierst, ist es wichtig, auf Zeit zu spielen. So fällt der Wert der Erpressung und im Hintergrund kann ein Restore ablaufen.

Es ist auch wichtig, das System nicht nur wiederherzustellen, sondern auch mögliche Sicherheitslücken zu schließen. Deshalb kann die Kommunikation mit dem Erpresser eventuelle wichtige Informationen verraten.

Wenn es kein Konzept für die Wiederherstellung gibt, dann solltest du in der Kommunikation mit dem Erpresser nicht auf deren Forderungen eingehen. Spiel lieber auch hier auf Zeit.

Der Angreifer weiß wahrscheinlich nicht mal, wie das Backupkonzept aussieht. Und selbst wenn er es wüsste, könntet ihr immer noch behaupten, dass die Datei von Magnetbändern wiederhergestellt werden kann (nur als Beispiel).

Hierbei kann dann die Forderungen gegen den entstandenen Schaden gegengehalten werden und behaupten, wieso sollt ein hoher Betrag bezahlt werden, wenn der Ausfall und die Wiederherstellung kostengünstiger ist?

Außerdem kann man nicht garantieren, dass die Daten entschlüsselt werden können. Das würde zwar der Reputation und dem Vertrauen des Angreifers schaden, aber sicher ist das nicht. Die Angreifer haben ein Ziel, das sie erreichen wollen. Dafür müssen sie in der Vergangenheit glaubhaft Daten entschlüsselt haben. Sonst könnten sie bei der Verhandlung weniger Druck aufbauen.

Fragt nach was BTC/Bitcoins sind, sei naiv dabei. Die Erpresser bieten einen guten Support an, um an das Geld des Unternehmens zu gelangen. Der Angreifer oder Erpresser muss dann beweisen, dass er in der Lage ist, Dateien zu entschlüsseln. Du entscheidest, welche Dateien du entschlüsseln willst und welche du vom angegriffenen System an den Erpresser überträgst.
Wenn du Glück hast, bekommst du eine Liste des "File Trees" geschickt von der du auch die Datei wiederherstellen lassen kannst. Damit siehst du, welche Dateien betroffen sind.

Da alle die Bitcoin-Wallets eingesehen werden können und es keine Anonymität gibt, sollte man nie einen Wallet mit dem vollen Lösegeld benutzen. Die Erpresser sollen einfach sehen, dass sie nicht verarscht werden und dass Geld zur verfügung gestellt wird. Es kann auch gesagt werden, dass es noch etwas dauert, bis das restliche Geld dafür freigegeben wird.
Wenn man bei der Kommunikation vermittelt, dass man selber auf die Finanzabteilung und Buchhaltung angewiesen ist, kann man zusätzliche Zeit gewinnen.

Wenn der Erpresser behauptet, er würde die Daten an die Konkurrenz verkaufen, dann ist das nicht wahr. Denn die Mitbewerber wollen auf dem Markt nicht mit solchen Daten erwischt werden.

Wenn sich vorgestellt wird, es gibt nicht viele Mitbewerber und ausgerechnet baut einer dieser Mitbewerber, kurz nach dem Angriff, eine Technologie nach bzw. baut etwas was mit der Technologie zu tun hat, ist dies auffällig und kann dann ausgelegt werden, dass dieser Mitbewerber den Angriff in Auftrag gab.

Dieses Argument dient nur dazu, Druck aufzubauen. So kann man die angegriffene Partei zur Zahlung zwingen oder motivieren. Eigentlich bringt es dem Erpresser auch nichts, nur zu publizieren, weil er dann kein Druckmittel mehr hat und dann hat auch die angegriffene Partei Zugriff darauf.

Hackbutzen und Gruppen müssen auch ihren guten Ruf und ihr Image pflegen, so wie es bei einem kommerziellen Unternehmen der Fall ist. Wenn die Hackbutzen einen schlechten Ruf haben, sinkt die Bereitschaft zu zahlen, weil niemand ihnen vertraut.

Der Angreifer muss auch beweisen, dass die Daten abflossen. Das heißt also, dass dieser einen Angriff auf das System nachweisen muss. Wenn man Glück hat, erfährt man auch, wie der Angreifer ins System eindringen konnte. Diese Info ist wichtig für den eigenen Bericht und auch beim Restore, um zu sehen, wie das System komprimiert wurde und wie man es absichern kann.

Egal, was der Angreifer behauptet – wir können nicht garantieren, dass er die gestohlenen Daten nicht an Dritte weitergegeben hat. Zum Beispiel an Einrichtungen, die nah an der Regierung und bei einer Konfliktpartei angesiedelt sind.

Auch wenn das Geld da überwiesen wurde und die Daten entschlüsselt wurden, können wir nicht sicher sagen, ob das System noch kompromittiert ist. Die Angreifer kombinieren oft unterschiedliche Angriffe und Schädigungen, um vom eigentlichen Vorhaben abzulenken.

Was wird benötigt, wenn man von Ramsonware betroffen ist?

Ein Unternehmen sollte sich schon vorher Gedanken darüber machen, wie es reagieren würde, wenn die eigene Infrastruktur angegriffen wurde. Es ist besser, wenn es für so einen Angriff schon ein Konzept gibt, damit man ohne Panik die passenden Gegenmaßnahmen ergreifen kann.
Was wird also benötigt, wenn es bereits brennt?

Ein Wiederherstellungskonzept

Ein gutes Wiederherstellungskonzept besteht darin, dass nicht alle Daten verloren sind, sondern nur von wenigen Tagen, sodass der Betrieb schnell wieder einsatzfähig ist. Aus betriebswirtschaftlicher Sicht darf der Betrieb nicht stillstehen. Deshalb ist der Verlust von Daten der letzten Tage weniger schlimm als der Stillstand. Das Wiederherstellungskonzept besteht aus einer guten Backupstrategie. Und ein gutes Backup muss durchdacht sein.

Das Backup ist unveränderbar

Ein Backup sollte dem Write-Only-Konzept folgen. Das heißt, du darfst es nach dem Erstellen nicht mehr verändern oder löschen können. So stellst du sicher, dass du kein oder ein fehlerhaftes Backup hast.

Unabhängigkeit

Die Backups sollten auf eigener Infrastruktur betrieben werden und den Betrieb nicht verlassen. Online-Backups sind zwar eine gute Option, aber in einem Wiederherstellungskonzept

sollten sie im Betrieb griffbereit sein. Denn wenn es zu einem größeren Ausfall oder einem Angriff kommt und du nicht mehr Zugriff auf die Accounts hast, brauchst du die Offline Backups, um ein Restore durchzuführen. Egal, welche Infrastruktur du hast oder ob du eine Cloud-Lösung nutzt – du kannst einen Restore auf einer anderen Infrastruktur wiederherstellen und das in einem funktionierenden und nicht komprimierten Zustand. So kann das Unternehmen schnell wieder einsatzbereit sein und einen größeren wirtschaftlichen Schaden abwenden. Außerdem kann es die Forderungen der Erpresser ignorieren.

Isoliert

Die Berechtigungen für die Backups eines Wiederherstellungskonzepts dürfen nicht über die reguläre Gruppen- und Rollenverwaltung vergeben und verteilt werden. Am besten, du erledigst administrative Arbeiten nur vor Ort. Remote-Zugriff sollte verboten sein. Dann können auch keine dritten Personen auf die Backups zugreifen oder sie stehlen.

Versioniert

Backups sollten idealerweise inkrementell sein. Das heißt, dass nur die Änderungen übertragen werden. Bei absoluten Backups sollte, wenn es sich nicht vermeiden lässt, neue Snapshots die bestehenden Daten nicht verändern. Wenn ein Angreifer seine Schadsoftware schon vor der Ausführung hinterlegt hat, kann es nach einem Restore passieren, dass der Angreifer den Angriff nochmal durchführt.

Verifiziert

Du solltest den Datenrestore nicht nur einmal ausprobieren, sondern regelmäßig testen, um zu bestätigen, dass die

Wiederherstellung funktioniert und auch die Keys korrekt hinterlegt sind. Wenn du dein System nicht aus dem Backup wiederherstellen kannst, weil die Routine fehlt, und du nicht weißt, ob die Backups funktionieren, dann kostet dich das Zeit und Energie. Und das ist es, was die Erpresser wollen.

Überwacht

Es ist wichtig, die Integrität der Backups zu überprüfen. Denn die können ja aus verschiedenen Gründen mal schiefgehen. Die Speicherkapazitäten können voll werden, außerdem können Änderungen der API/ABI oder Netzwerkprobleme das Erstellen von Backups negativ beeinflussen und diese nicht komplett abschließen. Deshalb sollte man unbedingt checken, ob Backups oder Snapshots auch richtig erstellt werden.

Risikobassiert

Die Wiederherstellung des Geschäftsbetriebes sollte schnell vonstattengehen, damit das Unternehmen arbeitsfähig ist und sich nicht genötigt hält, den Erpresser zu bezahlen. In der BWL geht's halt vor allem um Geld und nicht so sehr um rationale oder logische Überlegungen. Deshalb sollten wir das Wiederherstellungskonzept mit den genannten Punkten erstellen und die Integrität verifizieren sowie in Routinen testen.

Forensische Arbeit

Sollte es zu einem erfolgreichen Einbruch ins System gekommen sein und die Daten sind nun komprimiert oder verschlüsselt, muss neben der Kommunikation mit den Erpressern und der Wiederherstellung des Systems, auch ein Team die forensische Arbeit tätigen, um in Erfahrung zu bringen

- Was hat der Angreifer auf dem System getan?
- Auf welche Daten konnte der Angreifer zugreifen?
- Gibt es weitere Hosts, auf die zugegriffen wurde?
- War und wenn ja wie war der oder die Userin bei dem Angriff involviert?
- Wie kam der Angreifer rein?

Dadurch wird sicher gestellt, dass es zu keinem erneuten Einbruch kommt, dass die Schwachstellen geschlossen werden und mögliche Beteiligte aufgedeckt werden.

Task Force

Wenn das Wissen im Unternehmen bleiben soll, muss es eine Task Force oder eine eigene Abteilung für die forensische Arbeit geben.
Hier muss man aber aufpassen, dass man nicht einfach Leute aus dem bestehenden Team nimmt, die schon voll ausgelastet sind. Die zusätzliche Arbeit würde die Task Force sonst im Tagesgeschäft belasten.

Eine forensische Arbeit dauert lange und kann nicht nebenbei gemacht werden. Deshalb leidet das Tagesgeschäft darunter.

Eine Task Force darf man nicht nur zusammenstellen, wenn der Schaden schon passiert ist. Sie muss auch währenddessen mit dabei sein und schon vorher nach Anomalien Ausschau halten.

Es ist ein Trugschluss und Marketingsprache auf die Menschen hereinfallen, welch weniger in der Materie bewander sind, dass mit Automatismen und Alghorhytmen (Neusprech KI) Probleme erschlagen werden können. Solche Werkzeuge können bestehende Sammlungen erweitern, aber die zusätzliche Datenmenge muss neben der regulären Arbeit auch noch bewältigt und verarbeitet werden.

Wir können also sagen, dass eine Task Force und eine Sicherheitsabteilung solche Arbeiten nicht nebenbei macht. Es ist also Personal nötig, das die Dienste überprüft und nach Anomalien Ausschau hält.

Angriffe können auch neu sein und die Tools, die die Systeme scannen, erkennen sie vielleicht gar nicht. Oder sie erkennen durch Shortcutting und Degeneration falsche Anomalien. Die Task Force muss dann die Automatismen korrigieren oder einfacher gesagt, zur Verwaltung der dieser "KI" degeneriert.

Beispiel:
Die automatische Auswertung der gesammelten Daten hat eine Anomalie im Traffik während der Nacht ergeben. Für kurze Zeit gibt es mehr ausgehende Datenverbindungen.
Das kann eine valide Arbeit auf dem Dateisystem sein, aber es kann auch ein Anzeichen für einen Datenabfluss sein.
Werkzeuge können durch die Auswertung der Daten über den Vorfall informieren, jetzt das Personal aus dem Tagesgeschäft herausziehen und darauf anzusetzen führt dazu, dass

bestehende Aufgaben liegen bleiben und je nach Schwere der Situation der eigentliche Betrieb nicht vorangeht, bis die forensische Arbeit abgeschlossen ist.

Wenn ein Vorfall zu einer Bestätigung einer Kompromittierung führt, dann folgt die forensische Arbeit und Post Mortem Analyse.

Forensische Arbeit ist nicht einfach. Man muss vorsichtig und sorgfältig sein. Und manchmal dauert es ziemlich lange, je nachdem, wie schwer der Vorfall ist. Oft wird dabei auch Druck aufgebaut, damit der normale Betrieb weiter läuft. Dadurch entstehen bei der forensischen Arbeit jedoch Stress, wodurch Fehler bei der Verarbeitung und Analyse sich einschleichen.

Die Angreifer müssen identifiziert werden. Außerdem müssen die ausgenutzten Lücken, die Werkzeuge der Angreifer und der verursachte Schaden analysiert werden. Und wir müssen die Restbestände der Angreifer finden und ein Protokoll des Ganzen erstellen. Durch Anti-Forensik und weitere Tricks können diese Informationen verdeckt werden oder zu falschen Mustern führen. Dadurch können Analysewerkzeuge durch Shortcutting auf falsche Schlüsse kommen, obwohl kein kausaler Zusammenhang besteht.

Wenn es plötzlich mehr Traffik gibt, kann das zum Beispiel durch das Verhalten der Anwendung oder des Kunden verursacht worden sein. Vielleicht wird ein Upload-Prozess gestartet, wenn eine bestimmte Situation eintritt. Es kann auch ein Angriff sein, der schon länger versteckt läuft und Daten sammelt. Der Angriff kann die Informationen dann auf ein

anderes System übertragen. Die Analyse dazu muss man sich genau anschauen, ohne dabei Daten zu manipulieren. Also darf man die Zeitstempel nicht durch Lese- und Schreibzugriffe verändern. So kann man keine Beweise verfälschen oder vernichten.

Wenn wir eine eigene Abteilung, ein eigenes Team oder eine Task Force dafür haben, sind die Kapazitäten da. Dann kann die reguläre Arbeit weiterlaufen und es müssen keine Kapazitäten vom Tagesgeschäft für eine unbestimmte Zeit abgezogen werden.

Fehler können geschehen

Es ist wichtig zu sagen, dass Fehler passieren können, auch wenn man sich richtig Mühe gibt. Eine forensische Arbeit kann eben keine hundertprozentige Auskunft geben. Man kann Informationen immer falsch auswerten oder übersehen. Das liegt vor allem an den Maßnahmen der Anti-Forensik. Die arbeiten so, dass die Arbeitenden einer falschen Spur folgen oder der Angriff nicht richtig erkennbar ist. Angreifer überladen das System mit Daten, um die Suche und Analyse zu erschweren. So gewinnen sie mehr Zeit, um ihre Spuren zu verwischen oder den Angriff länger aufrechtzuerhalten.

Auch einfache Fehler können auftreten, wenn man im Vorfeld Dateien anfasst und dadurch die Zeitstempel verändert, die angeben, wann welche Datei das letzte Mal geöffnet oder bearbeitet wurde.

Es ist auch möglich, dass der Angreifer Hinweise bekommen hat, dass er entdeckt wurde, wodurch er Beweise und Hinweise

mit einem Fire-And-Forget löscht oder sogar größeren Schaden anrichtet. Das kann passieren, wenn ein Admin oder Forensiker*in durch Übermotivation einen auffälligen Dienst beendet oder eine auffällige Datei gelöscht hat.

Die Grundsätzlichen Fragen

Die Task Force sollte sich vor der Forensik erst mal die folgenden Fragen stellen.

- Was hat der Angreifer auf dem System getan?
- Auf welche Daten konnte der Angreifer zugreifen?
- Gibt es weitere Hosts, auf die zugegriffen wurde?
- War und wenn ja wie war der oder die Userin bei dem Angriff involviert?
- Wie kam der Angreifer rein?

Root-Cause-Analayse

Im Fokus der Forensik stehen die Identifikation und detaillierte Betrachtung möglicher Schwachstellen, sowie Untersuchung der Verbreitung und Ausführung von Angriffsvektoren und Schadsoftware. Auch eine Analyse der Funktionsweise und allgemeine Struktur zu verstehen, ist Teil der Root-Cause-Analayse. Ein weiterer wichtiger Punkt bei der Analyse ist, herauszufinden, welche Mechanismen der Angreifer benutzt haben könnte, um sich dauerhaft im Netzwerk zu halten.

Time Line Gestalten

Aus den gesammelten Informationen während der forensischen Arbeit muss eine Timeline erstellt werden, damit durch eine chronologische Sortierung der Vorfall nachvollziehbar bleibt und somit ein Überblick geschaffen wird.
Die Timeline kann man hier tabellarisch aufbauen. Zum Beispiel so:

Timestamp oder fortlaufende ID	**Angriffsvektor**	**Ergebnis oder Aktivität**
01.01.1970	Bruteforce SSH	Login mit legitimen User

Logbuch

Ein Logbuch während der Analyse sorgt bei den Forensiker*innen dazu, dass jede Schritte der Arbeit protokolliert und nachvollziehbar sind. Diese Schritte sollten mit einer fortlaufenden Nummer und Zeitstempel protokolliert werden.
Dieses Protokoll dient nicht nur der Transparenz, sondern auch der Nachvollziehbarkeit, was auch bei einer Beweislast vor Gericht herhalten muss.

ID	Timestamp	Aktivität	Ausführende Person
001	01.01.1970 13:12	Abbild der SSD mittels dd	Name, Vorname

ID	Timestamp	Aktivität	Ausführende Person
002	01.01.1970 13:37	Abbild in Kali Linux Live Medium eingebunden	Name, Vorname

Mögliche Vorgehensweise

Angreifer können durch eine niedrigschwellige Hürde in ein System eindringen. Ein Beispiel hierfür ist der Angriff durch Phishing-Mails.

Eine weitere Art des Angriffs ist es, durch Brute Force Zugang zu erlangen. Dieses Vorgehen ist meistens nicht erfolgreich, es sei denn, das System oder die Benutzer verwenden Standard- oder schwache Passwörter. Auch das Fehlen von Sicherheitsmaßnahmen, wie ein nicht vorhandenes Fail2Ban, begünstigt Brute-Force-Angriffe.

Gezielte Angriffe gehen eher auf Schwachstellen einer Anwendung, zum Beispiel ungepatchte Systeme. Als Beispiele sind VPN-Server zu nennen, die für Angriffe anfällig werden oder deren Verifikationen umgangen werden können. Eine Analysequelle könnte hierbei die Zugriffslogs sein, die abweichende IPs anzeigen. Auffällige IPs sind beispielsweise solche von nicht inländischen Providern oder solche, die sich außerhalb der bekannten Netze befinden. Die IP-Adressen müssen nicht zwangsläufig aus Russland oder China stammen, da die Angriffe auch von gekaperten Hosts kommen können.

Beliebt ist auch, mittels gestohlener Kreditkartendaten Rechenleistung in der Cloud zu erwerben und damit dynamisch die IPs zu rotieren.

Nach der Analyse der Zugriffslogs und des möglichen Eintritts ins System muss dieses auf Schwachstellen überprüft werden, um aus der Perspektive der Angreifer den möglichen Zugriff zu realisieren.

Abschließend sollte geprüft werden, ob es zu einem Datenabfluss kam. Hierzu sollte der ausgehende Traffik überprüft werden. Wird mehr ausgehender Traffik protokolliert? Gibt es Hinweise auf einen Upload? Steht etwas im Journal oder in den Logs? Gibt es auffälligen Traffik auf einem bestimmten Port?
Wurden Tools nachinstalliert, die nicht zum regulären Toolset gehören?

Es sollten auch Kommunikationskanäle wie Blogs, Telegram-Kanäle oder Foren der Angreifer beobachtet werden. Auch Tauschbörsen im sogenannten Darkweb werden von den Angreifern genutzt.

Wenn keine Erkenntnisse erlangt wurden, bedeutet dies nicht, dass keine Daten abgeflossen sind, sondern nur, dass keine Hinweise auf solche Fakten entdeckt wurden, wodurch die Wahrscheinlichkeit sinkt.

Anti-Forensik

Angreifer können mit Anti-Forensik Systeme so manipulieren, dass die eigentlichen Merkmale untergehen oder die forensische Arbeit erschwert wird.

Durch einen Mangel an Kapazitäten oder Personal kann dem Angreifer bewusst werden, dass er durch die Verschleierung von Anomalien Zeit gewinnen kann. Auch das Hinterlegen von falschen Fährten kann Administrator*innen ablenken.

Hierbei können falsche Muster greifen, Dateien mit auffälligen Namen können den Fokus der Forensiker*innen auf eine falsche Fährte lenken. Auch Compressed Archive Bombs sind nach wie vor beliebte Mittel, um Zeit zu gewinnen.

Dateisysteme können auch mit Dateien geflutet werden, um die Suche nach auffälligen Dateien zu erschweren. Ein manipuliertes Office-File könnte sich in einem Verzeichnis mit vielen anderen Dateien befinden. Die forensische Suche wird somit verlangsamt, da jede Datei überprüft werden muss. Auch bei einem Scan muss jede Datei angefasst und der Hash geprüft werden.

Auch können Inhalte Usern untergejubelt werden, wodurch unschuldige Dritte ins Fadenkreuz geraten können.

Dabei geht es den Angreifern nicht um eine 100-prozentige Verschleierung, sondern darum, die Ermittlung zu erschweren, zu verlangsamen und Steine in den Weg zu legen.

Manche Schadsoftware kann erkennen, ob ein Betriebssystem in einer Virtualisierung läuft, und versteckt sich oder wird nicht ausgeführt.

Die Angreifer können ebenso die Werkzeuge der Forensiker*innen angreifen oder torpedieren, sodass falsche Informationen ausgegeben werden, beispielsweise durch Ausnutzen von Bugs.

Wenn der Angriff gut durchdacht ist, werden Logdateien systematisch manipuliert, sodass die Informationen der Angreifer verschleiert werden. Eine weitere Möglichkeit ist, die Logdateien vollständig zu entfernen, was jedoch viel Aufmerksamkeit erregt.

Vorgehen der Angreifer

In der Vorstufe wird sich der Angreifer manuell oder automatisiert zunächst einen Überblick verschaffen und Informationen sammeln. Dabei ist das Footprinting die erste Phase und dient der Prüfung des Systems. Dabei wird der Zielbereich grob festgelegt, die IP-Range bestimmt und die erreichbaren Dienste geprüft. Durch die Erfragung gegen die Ports wird ermittelt, welche Software in welcher Version eingesetzt wird. Whois bietet Informationen darüber, wo sich welcher Host befindet und von wem er betrieben wird. So kann beispielsweise durch eine einfache Whois-Abfrage festgestellt werden, ob sich der Host bei OVH, Hetzner, Netcup und Konsorten befindet. DNS-Abfragen bieten die Möglichkeit, weitere Server und Informationen in Erfahrung zu bringen. Auch die TXT-Records sind hierbei interessant. Ebenso ist ein Blick auf ein SSL-Zertifikat interessant. Wenn dieses für mehrere Dienste genutzt wird, muss es auch alle Aliases und

FQDNs beinhalten. Dadurch können weitere Server und Dienste in die Sammlung des Angreifers aufgenommen werden.
Mithilfe dieser Informationen kann der Angreifer die Netzinfrastruktur untersuchen und eine Topologie erstellen beziehungsweise dieses Netz nachzeichnen. Aktive Hosts werden dann mittels Ping-Sweeps geprüft.

Der Angreifer wird mit den gesammelten Informationen jedoch nicht den eigentlichen Angriff starten, sondern das System zunächst auf Schwachstellen testen und prüfen, ob mögliche Zugriffe erhalten werden können.

Sollte ein Angriff möglich sein, werden Hintertüren offen gehalten, damit nach dem Schließen mittels Patches und Updates ein Angriff nicht mehr unterbunden werden kann. Das Patchen und Updaten kann dabei zufällig erfolgen und muss nicht unbedingt mit dem Entdecken der Angreifer zusammenhängen.

Danach werden die Spuren verwischt, die Logdateien geleert und die Schadsoftware verschleiert.

Täterprofil

Ein Täterprofil ist deshalb von Interesse, um die Motivation eines Angriffs zu ermitteln. Das Auffinden von Schadsoftware und deren Beseitigung ist Teil der gesamten Arbeit. Es muss auch in Erfahrung gebracht werden, weshalb ein Angriff stattfand. Kam dieser aus dem Unternehmen? Wurde das System kompromittiert, weil eine Person mit privilegierten Berechtigungen kooperiert hat? Wurde diese Person von einer

anderen Stelle zu dieser Tat motiviert? Kam der Angriff von außerhalb? Ging es um den Schaden oder um eine Erpressung, um an Geld zu gelangen? Nicht alle Angriffe verfolgen ein monetäres Interesse. Viele sind politisch motiviert oder dienen der Spionage. Im Täterprofil sollen deshalb die Motivation und die Gründe in Erfahrung gebracht oder eingeschätzt werden.

Erkenntnisse sammeln

Hinweis: Für manche Analysen und Prozesse ist es ratsam, zwei Werkzeuge zu benutzen, die das gleiche Ziel verfolgen. Denn die Ergebnisse könnten durch den Angreifer verfälscht worden sein oder die Programme könnten unterschiedliche Kompatibilitäten aufweisen und somit auch unterschiedliche Ergebnisse anzeigen. Wichtig ist, auch diese Unterschiede zu protokollieren.

Zu beachten ist auch, dass Vermutungen keine Beweise sind. Jedoch kann man diesen nachgehen, um zu prüfen, ob sich Fakten und Beweise hinter einer Vermutung befinden.

Liste flüchtiger Dateien

Bei flüchtigen Dateien handelt es sich um Daten und Informationen, die nur solange vorhanden sind, wie das System aktiv ist bzw. mit Netzspannung versorgt wird. Die interne Uhr eines Computers funktioniert beispielsweise nur, solange diese mit Strom versorgt wird. Ist die Stromversorgung unterbrochen, hört die Uhr auf, die Zeit hochzuzählen, und kann beim nächsten Start einen falschen Zeitstempel anzeigen.

Deshalb ist es wichtig, alle flüchtigen Daten zu sichern, solange diese noch abrufbar sind.

Prozesse

Die Liste der aktiven Prozesse sollte vor dem Herunterfahren gespeichert werden, um zu jedem Zeitpunkt nachvollziehen zu können, welche Prozesse aktiv waren. Dies kann in unixoiden Systemen mittels des Befehls `ps` aufgerufen und als Textdatei gespeichert werden.

Mit dem Befehl `$ ps auxf > /tmp/ps.txt` werden alle aktiven Prozesse als Baumstruktur aufgelistet und der jeweilige Benutzer der Prozess-ID angezeigt. Alternativ kann anstelle des ausgeschriebenen Users die PPID angezeigt werden:
`$ ps ajxf`

Sockets und Ports

Um alle offenen Sockets in Erfahrung zu bringen, gibt es mehrere Wege. Der einfachste ist, die Informationen aus dem Verzeichnis /proc mittels cat zu lesen.
`$ cat /proc/net/{tcp,udp}` Diese Informationen sind jedoch zumeist nicht leserlich. Eine Alternative ist das Tool `ss`, welches alle aktiven Sockets tabellarisch anzeigt. Mit dem Befehl `$ ss -a` werden alle belegten Sockets angezeigt, während mit dem Befehl `$ ss -alpn` alle Prozesse angezeigt werden, die genutzten Ports nicht in Namen ändern und der Prozess, der den Socket nutzt, angezeigt wird.

Aktive User

Es kann interessant sein zu wissen, wer alles aktuell auf dem System angemeldet ist. Dies kann mit dem Befehl `$ w` angezeigt werden.

Offene Verbindungen und Dateien

Es ist ratsam, sich die Information einzuholen, welche anderen Systeme aktuell Zugriff auf den betroffenen Host haben. Dies gilt nicht für Systeme, die mittels Automount oder via Sockets/Ports immer Zugriff auf das System haben. Es könnte zum Beispiel gerade eine Synchronisation oder Migration gestartet sein, wodurch andere Hosts betroffen wären. Dies kann mit dem Befehl `$ arp -n` angezeigt werden.

Aktuelle Verbindungen von Anwendungen wie Firefox oder Thunderbird können mit dem Befehl `$ lsof -P -i -n` angezeigt werden.

Wird der Befehl `lsof` ohne Parameter oder Argumente ausgeführt, werden alle offenen Dateien angezeigt, zum Beispiel alle aktuell genutzten Bibliotheken in `/lib` oder `/usr/lib`.

Caches

Die Caches von Anwendungen sollten gesichert werden, damit diese bei einem Neustart der Anwendung oder des Hosts nicht entfernt werden. Die Pfade variieren hierbei je nach Installation und Anwendung.

Arbeitsspeicher und Swap

Aus Sicherheitsgründen kann der genutzte Arbeitsspeicher seit einiger Zeit nicht mehr direkt gedumpt werden. Hierzu wird ein Kernelmodul namens LiME (https://github.com/504ensicslabs/lime) benötigt, welches eine Brücke schlägt. Mittels dieses Kernel-Moduls können Werkzeuge auf die Daten im Arbeitsspeicher zugreifen.

Informationen zur aktuellen Nutzung des Arbeitsspeichers können mit dem Befehl `$ cat /proc/meminfo` angezeigt werden. Swaps müssen keine Partition sein, sondern können auch eine Datei auf einem Dateisystem sein. Eine Liste der aktiven SWAPs kann mit dem Befehl `$ cat /proc/swaps` angezeigt werden.

Dateisysteme und Datenträger

Eine Liste der aktuell eingebundenen Dateisysteme kann mit dem Befehl `$ df -h` angezeigt werden. Eine ausführliche Liste aller eingebundenen Systeme, wie `dev` oder `gvfsd-fuse`, wird in `/proc/mounts` gelistet.

Die Liste aller angeschlossenen Datenträger am System kann mit dem Befehl `$ fdisk -L` angezeigt werden.

Alternativ kann auch der Befehl `$ lsblk -p -f -l` genutzt werden, um eine tabellarische Ansicht mit Dateisystem und deren Mountpoints anzuzeigen.

Von Interesse ist auch, welche Laufwerke wie eingebunden werden sollen. Deshalb muss die Datei `/etc/fstab` ausgelesen und gesichert werden.

System Information

Auch die Version des aktuell genutzten Linux-Kernels und die Version des Compilers sollten als Notiz gespeichert werden. Dies kann durch den Befehl `$ cat /proc/version` ausgelesen werden.

Die Liste der Kernel-Command-Line-Parameter, mit welchen das System gestartet ist, kann durch `$ cat /proc/cmdline` in Erfahrung gebracht werden.

Die derzeit aktiven Module des Linux-Kernels können aus `$ cat /proc/modules` ausgelesen werden.

Die aktuell genutzten Umgebungsvariablen sollten gesichert werden. Dies gelingt mit dem Befehl `$ env`.

Netzwerk

Sichere alle derzeitigen Informationen zum Netzwerk deines Computers. Erfasse, welche Interfaces bestehen, welche IP-Adressen diesen zugewiesen sind und welche MAC-Adressen diese haben. Führe dazu den Befehl `$ ip a` aus. Auch die aktuell genutzten Routen sollten gesichert werden. Dies kann mit dem Befehl `$ ip route show` oder `$ netstat -rn` in Erfahrung gebracht werden.

DNS

Ein Angreifer könnte die Hosts-Datei des Systems manipuliert haben, um Anfragen gegen Domains umzuleiten. Prüfe und

sichere deshalb auch die Datei `/etc/hosts` des Systems. Ebenso kann ein manipulierter Nameserver genutzt werden, weshalb die Ausgabe von `/etc/resolve.conf` ebenfalls gesichert werden sollte. Wenn das System anders konfiguriert ist und keine `/etc/resolve.conf` nutzt, beispielsweise wenn Systemd-Resolved konfiguriert wird, muss diese Konfiguration entsprechend ausgelesen und gesichert werden.

Users

Ein Angreifer könnte sich durch einen Benutzer am System eine Hintertür erstellt haben, über die er privilegierte Zugriffe erhalten könnte. Deshalb sind die Dateien `/etc/passwd` und `/etc/shadow` von Interesse.

Skript zum Sammeln von Informationen

Mit diesem Skript kann eine Liste mit Informationen aus `/proc/$PID` der aktuellen, bestehenden Prozess-IDs erstellt werden:

```
ls /proc | sort -n | grep -v "[a-z,A-Z]" |\
while read PID; do
echo "Prozess ID $PID:"
cat /proc/$PID/cmdline
cat /proc/$PID/environ
cat /proc/$PID/maps
cat /proc/$PID/stat
cat /proc/$PID/statm
cat /proc/$PID/status
cat /proc/$PID/mem
ls -ld /proc/$PID/root
ls -ld /proc/$PID/cwd
ls -ld /proc/$PID/exe
ls -ltra /proc/$PID/fd/
echo
"-------------------------------------------------";
done
```

Systemduplikat

Es sollte vermieden werden, auf dem betroffenen System direkt zu arbeiten. Stattdessen sollte ein bitgenaues Abbild des Systems erstellt werden. Unter unixoiden Systemen wird hierfür das Programm `dd` genutzt. Bei Virtualisierungen und Clouddiensten gibt es Möglichkeiten, das Image herunterzuladen oder zu duplizieren bzw. einen Snapshot zu erstellen.

Das Abbild des betroffenen Systems sollte in einer abgekapselten Umgebung eingebunden werden, das entweder gar keinen Internetzugriff aufweist oder jeglichen Traffic nach außen zu einem Honeypot leitet.

Dadurch wird verhindert, dass die Schadsoftware mit dem Command-and-Control-Server kommuniziert oder der Angreifer mittels Remote Execution darauf reagieren kann, um beispielsweise Gegenmaßnahmen zu ergreifen oder weitere Daten zu stehlen.

Darüber hinaus kann immer wieder zum kompromittierten Zeitpunkt gestartet werden, um die Daten zu vergleichen.

Angreifer können ihre Schadsoftware jedoch auch so gestalten, dass sie erkennt, dass sie sich nicht mehr im Ursprungssystem befindet beziehungsweise, dass sich die Umgebung geändert hat. Dadurch kann die Schadsoftware ihren weiteren Dienst verweigern oder sich selbst verstecken. Eine solche Erkennung basiert darauf, dass sich das Hostsystem verändert hat, eine andere Virtualisierung aufweist oder, falls es nicht zuvor virtualisiert wurde, eine erkannt wird. Auch die Erreichbarkeit des System And Controll Center kann die Aktivitäten der Software beeinflussen.

Das Duplikat kann aus unterschiedlichen Gründen während des Betriebs oder im ausgeschalteten Modus erstellt werden. Beispielsweise, wenn die Schadsoftware nur im Arbeitsspeicher liegt und somit spätestens nach einem Neustart nicht mehr vorhanden ist. Umgekehrt kann die Erstellung eines Duplikats im laufenden Betrieb jedoch auch Beweise manipulieren.

Dateisystem-Metainformationen

Die Metadaten eines Dateisystems können wichtige Hinweise und relevante Informationen beinhalten. Von Interesse sind dabei die Zeitstempel, die angeben, wann zuletzt auf eine Datei zugegriffen oder diese ausgeführt wurde, sowie die Berechtigungen, die diese Dateien hatten.

So können beispielsweise die Berechtigungen von Benutzer und Gruppe sowie die Lese- und Ausführberechtigung Hinweise auf Schwachstellen oder die Ursache für einen Angriff liefern.

Ein sehr simpler Angriff wäre beispielsweise, wenn durch ein automatisches Deployment eine Init-Service-Datei erstellt wird, die von einem unprivilegierten Benutzer bearbeitet werden kann.

Jeder Datei sind drei Zeitstempel zugeordnet. Linux speichert diese im Unix-Zeitformat, das die Sekunden seit der Epoche misst. Die drei Zeitstempel werden üblicherweise als atime, ctime und mtime bezeichnet.

- mtime
  mtime ist am gebräuchlichsten und oft auch am nützlichsten. Sie gibt die modifizierte Zeit an. Das ist der Zeitpunkt, zu dem der Inhalt der Datei zuletzt auf die Festplatte geschrieben wurde.

- Ctime
  ctime verfolgt Metadatenänderungen wie Eigentum und Berechtigungen. Es wird aber auch aktualisiert, wenn sich der Inhalt der Datei ändert, sodass es immer so

aktuell ist wie die mtime.

- Atime
  atime zeigt den letzten Zugriff auf eine Datei.

- Etime
  Die elapsed time gibt das Alter eines Prozesses an.

- Ownership
  Welchem Benutzer und welcher Gruppe gehört die Datei?

- Permission
  Welche Berechtigung hat der Benutzer und die Gruppe? Lesen, Schreiben, Ausführen.

Erste Schritte zur Sicherstellung

Die flüchtigen Daten müssen gesichert werden, bevor es zu einem Neustart oder Herunterfahren des Systems kommt und diese damit den Speicher verlassen.

Das System sollte sich am besten im ausgeschalteten Zustand befinden. Es gibt Situationen und Ausnahmen, in welchen die forensische Arbeit während des Betriebs stattfinden soll, aber der Regelfall sieht vor, dass weder das Betriebssystem aktiv ist, noch das Dateisystem eingebunden ist. Dies verhindert eine versehentliche Manipulation der Daten.

Alle Personen, die aktuell Zugriff auf das System haben, müssen entfernt bzw. distanziert werden, damit sie die Arbeit

nicht negativ beeinflussen oder Spuren absichtlich oder versehentlich verwischen.

Der Standort des Systems sollte protokolliert werden, damit auch im Nachgang bekannt ist, welche Möglichkeiten mit welchen Zugriffen vorhanden waren.

Befindet sich das System im Stand-by-Modus, beispielsweise ein Notebook oder ein Desktop-Arbeitsplatz, soll dieses System ohne geweckt zu werden abgeschaltet werden.

Das Gerät soll vom Netzwerk getrennt werden, um zu verhindern, dass durch ein Versehen Daten abfließen oder eine Kommunikation mit dem Angreifer stattfindet. Dies soll auch verhindern, dass weitere Systeme im Netzsegment betroffen werden.

Gibt es Besonderheiten zu dem Gerät oder System? Diese sollten in Erfahrung gebracht werden, damit diese Besonderheiten berücksichtigt werden können.

Ebenfalls müssen Passwörter und Konfigurationen zu dem System in Erfahrung gebracht werden.

Bis zum Abschluss der Forensik

Alle betroffenen Accounts müssen gesperrt werden. Zugriffe, die wieder gewährt werden müssen, um den Betrieb aufrechtzuerhalten, sollen mit neuen, starken Passwörtern versehen werden und unter Beobachtung stehen. Ist die Quelle des Angriffs lokalisiert, soll der ISP weitere Informationen zur

Quelle bereitstellen. Dies kann beispielsweise durch Staatsbehörden erfolgen.

Netzwerk-Segmentierung

Bei der Überprüfung des Systems sollte eine Netzwerksegmentierung stattfinden, bei der geprüft wird, welche weiteren Systeme direkten oder indirekten Zugriff auf das betroffene System hatten. Dies geschieht am besten während der Isolation des betroffenen Systems. Dabei sollte das Netzwerk in drei Kategorien eingeteilt werden:

Rot:
Dies ist die kompromittierte Zone. Alle Dienste in dieser Zone sind direkt betroffen oder können betroffen sein. Diese Dienste und Systeme dürfen nicht mit der nächsten Zone interagieren, da diese sonst ebenfalls gefährdet ist, kompromittiert zu werden.

Gelb:
Hierbei handelt es sich um Netzwerksegmente, die eine Vertrauensbeziehung zur roten Zone pflegten. Sie müssen von der roten Zone getrennt und zumindest mit Scannern auf eventuelle Angriffe geprüft werden.

Grün:
Hierbei handelt es sich um ein isoliertes Netzwerksegment, das mit der roten Zone nicht im direkten Kontakt stand und somit weiterbetrieben werden kann. Um Systeme in die grüne Zone zu bewegen, müssen diese ein gehärtetes System aufweisen und nach einem Angriff neu bereitgestellte Dienste bieten und die maximal höchste Sicherheit gewährleisten.

Kompromittierte Systeme können selbst nach dem Aufräumen weiterhin Hintertüren aufweisen oder Schadsoftware beinhalten.

Erstellen einer bitgenauen Kopie

Arbeite niemals direkt auf dem betroffenen System, sondern erstelle bitgenaue Kopien des Systems. Nutze hierfür die Software-Lösung dd:
`$ dd if=/dev/<Device>/<Partition> of=/path/to/image.dd bs=1M`.
Dies erstellt eine Kopie des Systems als Image, welches anderweitig eingespielt oder eingebunden werden kann. Es ist ratsam, mit einer Kopie der Kopie zu arbeiten, damit das betroffene System nicht immer herangezogen werden muss. Somit sollte Folgendes vorhanden sein:

- Betroffenes System
- main-image.dd
- copy_date-image.dd
- main-image.dd
- copy_date-image.dd
- usw.

Somit ist es immer möglich, aus dem main-image.dd die erste bitgenaue Kopie zu nehmen, sollte es während der Arbeiten zu einem Versehen kommen.

Das Tool dd ist auch in der Lage, via Netzwerk und SSH ein Image zu erstellen, indem Pipes genutzt werden.

```
$ ssh user@host "dd if=/dev/<device><partition> | gzip -1 -" | dd of=/local/path/to/image.gz
```

Bei virtuellen Maschinen, die sich im Cloud-Kontext befinden, bieten die Anbieter auch die Möglichkeit, diese Images herunterzuladen oder Snapshots zu erstellen. Clouddienste, die auf OpenStack aufbauen, bieten hierfür API-Lösungen oder ein Webfrontend. Bei weniger modernen Systemen kann mit dem Anbieter in den Austausch getreten und um das Abbild gebeten werden. Prüfen Sie auch in der eigenen Infrastruktur, ob solch eine Option besteht. VMware bietet solche Funktionalitäten zum Beispiel an. Ebenso kann Proxmox solche Funktionen zur Verfügung stellen.

Würdigung des Umfelds

Erfahre, wer alles Zugang zum System hatte. Jede Person kann den Angreifer hierbei absichtlich oder versehentlich unterstützt haben.

Können Spuren durch Dritte entstanden sein?

Existieren Beweise, welche die Aussagen bestätigen oder widersprechen?

Gibt es Kommunikationskanäle wie Chats oder Social Media, die auf die oder den Verdächtigen zurückzuführen sind?

Post Mortem Analyse

Die Post-Mortem-Analyse findet auf einem Abbild des Systems statt. Während der Analyse können Backups eingespielt und das System sowie das Netzwerk gehärtet werden, um den Betrieb zu gewährleisten.

Da das System kompromittiert ist, können auch die Analyse-Tools manipuliert sein, sodass gewohnte Befehle nicht korrekt funktionieren oder Informationen verschleiert werden. Hierbei handelt es sich um ein Anti-Forensik-Verfahren, bei dem Angreifer den Angriff verschleiern oder sich decken wollen. Deshalb sollte das betroffene System in einer Live-Image-Umgebung eingebunden werden, in der die Werkzeuge und Kommandos nicht manipuliert wurden. Hierzu kann entweder ein eigenes Image erstellt oder Kali Linux genutzt werden.

Beispiel
Auf dem System wurde das Tool `cat` durch eine manipulierte Variante ausgetauscht, die auf die gleiche Weise funktioniert, aber Spuren und Hinweise nicht anzeigt.

Erstelle einen Suchindex aller Dateien und prüfe alle Dateien mittels einer Hash-Datenbank auf Ungereimtheiten. Hierbei können harmlose Dateien ausgeblendet werden. Solche Listen können beispielsweise bei NIST als Datenbank bezogen werden.

Eine Kategorisierung von Dateien nach Typ erleichtert die forensische Arbeit.

Da nicht bekannt ist, ob sich die Schadsoftware oder die Spuren vernichtet wurden, sollten die Dateien wiederhergestellt werden. Die Wiederherstellung mittels File Carving erfolgt unabhängig vom Dateisystem. Dazu wird der rohe Datenstrom des Speichermediums nach charakteristischen Zeichenfolgen, wie einer magischen Zahl, oder nach anderen typischen Kopfdatenstrukturen bekannter Dateiformate durchsucht.

Prüfe die Cronjobs, Systemd-Timer oder die Queue von at nach verdächtigen Handlungen.

Wenn die Schadsoftware aufgefunden wurde, prüfe den Code nach Spuren. Können daraus Erkenntnisse gewonnen werden, die auf den oder die Verdächtigen zurückzuführen sind?

Zeitstempel-Analyse

Bei der forensischen Arbeit am System sind die Zeitstempel von Relevanz, um nachvollziehen zu können, was wann geschah. Es muss auch darauf geachtet werden, dass die Zeitstempel in Logs und Journals einheitlich sind bzw. auf Unterschiede hingewiesen wird, da die Zeitzonen sonst die Interpretation beeinflussen können, beispielsweise bei Sommer- und Normalzeit. Dies kann die chronologische Reihenfolge beeinflussen und somit die forensische Arbeit behindern.

Angreifer können Daten und Logs manipulieren, um Spuren zu verwischen oder auf eine falsche Fährte zu locken. Dies ist jedoch zeitintensiv und teilweise komplex, sodass diese Manipulation vergessen wird oder nicht sauber durchgeführt wurde. Auch die Metadaten werden nicht immer berücksichtigt. Das stupide Löschen ist effizienter, sorgt aber für den Hinweis, dass jemand absichtlich Informationen zerstört hat.

Diese Metainformationen können beispielsweise mittels `$ stat` aufgerufen werden, welches die MAC-Timestamps ausgibt. Diese Zeitstempel werden jedoch schnell aktualisiert,

wodurch versehentlich Informationen vernichtet werden können.

Deshalb müssen vor dem Öffnen einer Datei immer die MAC-Timestamps eingeholt werden, damit diese Informationen protokolliert werden können.

Auslagerungsdateien

Die Analyse von Auslagerungsdateien ist von großem Interesse. Swapfiles und Partitionen beinhalten oft noch Informationen, die aus dem Arbeitsspeicher ausgelagert wurden und derzeit nicht benötigt werden. Dabei können sich sowohl vom System als auch vom Angreifer stammende Daten sowie noch aktive Schadsoftware in der Auslagerung befinden. Die Auslagerungsdatei wird wie der RAM nach dem Neustart geleert. Es ist somit lohnenswert, ein Abbild des aktuellen Swaps zu haben oder im Swapfile nach etwas zu suchen.

Binärdateien analysieren

Auffällige Binärdateien können modifizierte Versionen sein, die um einen Schadcode erweitert wurden. Diese Binärdateien sollten in einer gesicherten Umgebung betrachtet und der Hashwert sollte verglichen werden. Auch mittels des Befehls `$ file` können Informationen ausgegeben werden. Mit dem Befehl `$ string` können weitere Informationen über die Binärdatei ausgegeben werden, um diese im Internet zu recherchieren.

Eine Laufzeitanalyse eines Prozesses zeigt in einer abgekapselten Umgebung, was das Programm tut. Hierzu können die Befehle `$ strace` oder `$ truss` genutzt werden.

Tooling

AVML

AVML (Acquire Volatile Memory for Linux) ist ein portables Werkzeug zur Erfassung flüchtiger Speicher für Linux, das in Rust geschrieben wurde und als statische Binärdatei bereitgestellt werden soll. AVML kann verwendet werden, um Speicher zu erfassen, ohne dass die Ziel-OS-Distribution oder der Kernel im Voraus bekannt sein müssen. Eine On-Target-Kompilierung oder Fingerprinting ist nicht erforderlich.

chrootkit

Chkrootkit (Check Rootkit) ist ein Unix-basiertes Programm, das Systemadministratoren dabei unterstützt, ihr System auf lokale Anzeichen bekannter Rootkits zu überprüfen. Es handelt sich um ein Shell-Skript, das gängige UNIX/Linux-Tools wie die Befehle strings und grep verwendet, um Kernsystemprogramme nach Signaturen zu durchsuchen. Zudem wird ein Traversal des Dateisystems /proc mit der Ausgabe des Befehls ps (Prozessstatus) verglichen, um nach Abweichungen zu suchen.

dd

dd ist ein Unix-Kommando, das zum blockorientierten Kopieren oder Konvertieren beliebiger Dateien dient. Die Größe jedes „Datenblocks” liegt üblicherweise zwischen einem Byte und einem Vielfachen der Blockgröße eines Dateisystems. Mit diesem Tool können Abbilder vom Dateisystem erstellt werden. `$ dd if=/dev/sda1 of=~/sda1.dd bs=1M`

find

Suche nach Namen von Dateien und Verzeichnissen auf dem Dateisystem, auch mittels regulärer Ausdrücke und der Option, Kommandos daran zu verbinden. `$ find <pfad> -iname "*.pdf" -type f -exec stat {} \;`

file

Mit dem Shell-Befehl file kann der Typ der in einer Datei enthaltenen Daten ermittelt werden.

fls

fls listet die Dateien und Verzeichnisnamen in einem Dateisystem auf. Es verarbeitet den Inhalt eines bestimmten Verzeichnisses und kann Informationen über gelöschte Dateien anzeigen. Beispiel: `$ fls ~/sda1.dd`.

foremost

Foremost ist eine freie Software zur Wiederherstellung von gelöschten, noch nicht überschriebenen Dateien oder Dateien aus beschädigten Dateisystemen mittels Carving. Foremost

sucht bekannte Anfangssequenzen und interpretiert dann die gesamte Sequenz bis zur zugehörigen Endsequenz als Datei. Neben einer Reihe eingebauter Datei-Erkennungsmuster können auch eigene definiert werden. Bei einer fragmentierten Datei wird bei einer pro Dateityp definierten maximalen Dateigröße abgebrochen. Foremost kann nur mit Dateien bis zu einer Größe von zwei Gigabyte umgehen.

gdb

GDB (GNU Debugger) ist ein UNIX-Programm und der De-facto-Standard-Debugger von Linux-Systemen. Er wurde vom GNU-Projekt entwickelt und bietet die üblichen Möglichkeiten zur Ablaufverfolgung wie Breakpoints oder die Ausgabe des Stacktraces. Darüber hinaus ermöglicht GDB ein Eingreifen in die Ausführung von Programmen. So können Benutzer beispielsweise die Variablen des Programms manipulieren oder Funktionen unabhängig vom normalen Programmablauf aufrufen. Ab Version 7.0 ist die Ablaufverfolgung nicht nur vorwärts, sondern auch rückwärts möglich (Reverse Debugging). Außerdem kann GDB mit Python und GNU Guile automatisiert werden.

hexyl

Hierbei handelt es sich um einen einfachen Hex-Betrachter, der im Terminal ausgeführt wird. Hexyl bietet ausschließlich Lesemöglichkeiten und kann Dateien nicht bearbeiten.

icat

Hierbei handelt es sich um einen einfachen Binärbetrachter, welcher im Terminal ausgeführt wird. Icat hat nur Lesemöglichkeiten und kann Dateien nicht bearbeiten.
In Verbindung mit `fls` kann icat Dateien aus einer bitgenauen Kopie (mit `dd` erstellt) lesen, ohne dass dieses Image eingespielt werden muss. Mittels `fls` wird somit die Inode-ID in Erfahrung gebracht und `icat` kann dann durch die Kombination aus der bitgenauen Kopie und der Inode-ID die Datei ausgeben, wie es bei einem regulären cat-Befehl der Fall wäre. `$ icat ~/sda1.dd 131437`

ifind

Anzeige des Inodes, der auf einen spezifischen Datenblock zeigt.
`$ ifind -f linux-ext4 ~/sda1.dd -n /grub`

ils

Auflistung aller Inodes einer Partition. `$ Ils -A ~/sda1.dd`

ldd

ldd (List Dynamic Dependencies) ist ein Dienstprogramm, das die Shared Libraries ausgibt, die von jedem auf der Kommandozeile angegebenen Programm oder jeder angegebenen Shared Library benötigt werden.

LiME

Ein Kernelmodul zur Erfassung des flüchtigen Speichers von Linux und Linux-basierten Geräten wie Android. Außerdem minimiert es die Interaktion zwischen Benutzer- und Kernel-Space-Prozessen während der Erfassung. Dadurch ist es möglich, Speichererfassungen zu erstellen, die forensisch fundierter sind als die anderer für die Erfassung von Linux-Speicher entwickelter Tools.

lsof

Das Programm „List Open Files" zeigt Informationen über geöffnete Dateien an. So kann mit der Option **p** und einer PID-Nummer angezeigt werden, auf welche Dateien und Ports dieser Prozess zugreift. Mit der Option **i** liefert lsof hingegen die Informationen, welcher Netzwerkdienst von welchem Anwender bzw. welcher PID benutzt wird.

mac-robber

Mac-Robber ist ein Ermittlungswerkzeug, das Daten von allozierten Dateien in einem eingebundenen Verzeichnis im Dateisystem sammelt. Die gesammelten Daten können dann mit mactime aus dem SleuthKit analysiert werden, um eine Timeline der Aktivitäten zu erstellen.
mac-robber baut dabei auf dem Werkzeug grave-robber auf.

mactime

Mactime erstellt eine ASCII-Timeline der Dateiaktivitäten auf der Grundlage der Ausgabe von fls: `$ fls -r -m / ~/sda1.dd > body.txt` und `$ mactime -b body.txt`.

md5deep

Bei md5deep handelt es sich um eine Suite, mit der sich MD5-Hashes für eine beliebige Anzahl an Eingabedateien berechnen und prüfen lassen. Dabei kann es Verzeichnisstrukturen rekursiv durchlaufen sowie durch bekannte Hashwerte gehen und dabei einen positiven oder negativen Abgleich durchführen.

md5sum

md5sum ist ein Computerprogramm, das 128-Bit-MD5-Hashes, wie in RFC 1321 beschrieben, berechnet und verifiziert. Der MD5-Hash fungiert als kompakter digitaler Fingerabdruck einer Datei. Wie bei allen Hash-Algorithmen dieser Art gibt es theoretisch eine unbegrenzte Anzahl von Dateien, die denselben MD5-Hash haben. In der realen Welt ist es jedoch sehr unwahrscheinlich, dass zwei nicht identische Dateien denselben MD5-Hash haben, es sei denn, sie wurden speziell mit demselben Hash erstellt.

mmls

Im Allgemeinen wird dies verwendet, um den Inhalt der Partitionstabelle aufzulisten und festzustellen, wo eine Partition beginnt. `$ mmls -t dos disk.dd`

netstat

Mithilfe von netstat können die Netzwerkrouten angezeigt werden `$ netstat -r`, die Interfaces mit MTUs `$ netstat -i`, sowie aufgebaute Verbindungen `$ netstat`.

nfdump

NFDump ist ein Netflow-Anzeige- und -Analyseprogramm. Es liest die Netflow-Daten aus den von nfcapd gespeicherten Dateien und verarbeitet die Flows entsprechend den angegebenen Optionen. Die Filtersyntax ist mit der von tcpdump vergleichbar und wurde für Netflow-Daten erweitert. Nfdump kann auch viele verschiedene Top-N-Flow- und Flow-Element-Statistiken anzeigen.

nm

„nm" ist ein Unix-Befehl, mit dem sich die Symboltabelle und ihre Attribute aus einer binären ausführbaren Datei auslesen lassen (einschließlich Bibliotheken, kompilierter Objektmodule, Dateien mit gemeinsam genutzten Objekten und eigenständiger ausführbarer Dateien).

nmap

Nmap ist ein kostenloser Portscanner, mit dem sich Hosts in einem Rechnernetz scannen und auswerten lassen. Der Name steht für „Network Mapper". Nmap wird in erster Linie für das Portscanning, also das Untersuchen der Ports eines Hosts, eingesetzt. Das Werkzeug wurde ständig erweitert und konnte sich vor allem durch seine aktiven Techniken für das OS-Fingerprinting – das Erkennen des eingesetzten Betriebssystems auf dem Zielhost – einen Namen machen.

Auch das Mapping von Umgebungen (Erkennen aktiver Hosts) ist möglich. Darüber hinaus lassen sich mit Nmap die hinter einem Port stehenden Dienste und deren Version teilweise auslesen. Nmap ist sowohl bei Angreifern als auch bei Administratoren sehr beliebt, da es sehr effizient und zuverlässig arbeitet. Es ist ein wichtiger Bestandteil bei der Netzwerkdiagnose und Auswertung netzwerkfähiger Systeme. Unter anderem wird es auch vom Vulnerability-Scanner Nessus zur Erfassung offener Ports eingesetzt. Nmap kann auch Bannergrabbing betreiben: `$ nmap -sV --script=banner <host>/<range>`. Dieser Vorgang ist zwar zeitaufwendig, liefert aber detaillierte Informationen zu den eingesetzten Softwares und Versionen, weshalb Nmap bei Forensikern und Angreifern gleichermaßen beliebt ist.

nslookup

Bei Nslookup handelt es sich um ein Werkzeug, um IP-Adressen einer Domain in Erfahrung zu bringen.

objdump

Objdump ist ein Befehlszeilenprogramm, mit dem sich Informationen zu einem Objekt auf Unix-ähnlichen Systemen anzeigen lassen. Wenn der Befehl verwendet wird, ruft er die Informationen einer Objektdatei ab, auch wenn der Quellcode nicht verfügbar ist. Daher kann es ein Debugging-Tool für Objektdateien sein, insbesondere bei der Arbeit mit Compilerprogrammen.

od

Das Unix-Kommando `od` dient zur Erstellung eines Dumps in verschiedenen, für Menschen lesbaren Formaten. Der Name leitet sich aus dem Akronym „Octal Dump“ ab, da der Befehl standardmäßig die Daten im Oktalsystem ausgibt. Neben dem oktalen System gibt od Daten optional auch im hexadezimalen, dezimalen System sowie in ASCII aus.

PEiD

Tool zur Erkennung von über 600 PE-Packern, -Cryptern und -Compilern in Binaries.

pcat

PCAT ist ein Programm ähnlich zu ZCAT, welches gepackte Dateien mittels „pack” lesen kann.

ps

ps (für Process Status) ist ein Unix-Kommando, das eine Liste aller Prozesse, die momentan laufen oder sich im Zombie-Status befinden, auf dem Bildschirm ausgibt.

Radare2 (r2)

Radare2, auch unter r2 bekannt, ist ein Framework für Reverse Engineering und Analyse von Binärdateien. Es besteht aus einer Reihe kleiner Dienstprogramme, die zusammen oder unabhängig voneinander über die Kommandozeile verwendet werden können. Es basiert auf einem Disassembler, der Maschinencode in Assemblercode konvertiert und dabei eine

Vielzahl von ausführbaren Formaten, Prozessorarchitekturen und Betriebssystemen unterstützt.

rkhunter

Der Rootkit Hunter ist ein Werkzeug, das nach Rootkits, Hintertüren und Exploits sucht. Dazu vergleicht er vorhandene Dateien anhand von Hashes mit kompromittierten Dateien, überprüft neu erstellte Ordner und Dateirechte, sucht nach versteckten Dateien und Strings in Kernelmodulen.

stat

Mit dem Befehl `stat` (von „status”) lassen sich die Zugriffs- und Änderungszeitstempel von Dateien und Ordnern anzeigen. Weiterhin werden Informationen zu Rechten, zum Besitzer und zur Gruppe sowie zum Dateityp ausgegeben. Durch Formatangaben kann die Ausgabe an die eigenen Bedürfnisse angepasst werden.

strace

Mithilfe von `strace` ist es möglich, die Systemaufrufe (System-Calls) eines Prozesses zu verfolgen. Dazu schaltet sich `strace` zwischen den Kernel und den Prozess und protokolliert die Aktivitäten. Wenn der Prozess einen Systemaufruf ausführt, zeigt `strace` den Namen, die Argumente und den Rückgabewert des Systemaufrufs an. Bei Signalen gibt `strace` den Namen des Signals aus. Strace ist ein Debugger und wird eingesetzt, wenn etwas nicht funktioniert oder wenn man verstehen möchte, was ein Programm tut.

strings

Der Befehl `strings` druckt im Wesentlichen die Zeichenketten druckbarer Zeichen in Dateien aus, um beispielsweise eingesetzte Bibliotheken einer Binärdatei in Erfahrung zu bringen oder auf Hinweise des Autors zu stoßen. `$ strings -n 10 /usr/bin/ccat` informiert uns beispielsweise über die genutzten Bibliotheken und darüber, dass das Programm mit einem Go-Compiler kompiliert wurde.

tcpdump

`tcpdump` ist eine freie Software zur Überwachung und Auswertung von Netzwerkverkehr. `tcpdump` arbeitet im Textmodus und wird über die Kommandozeile gesteuert. `tcpdump` ist für die meisten Unix-Systeme und Unix-Derivate wie AIX, BSD, Linux und Solaris verfügbar und wird von vielen Herstellern bereits im Grundsystem mitgeliefert. Das Programm liest Daten in Form von Paketen, die über das Netzwerk gesendet werden, und stellt sie auf dem Bildschirm dar oder speichert sie in Dateien. Durch die Umstellung eines Netzwerkadapters in den Promiscuous-Modus ist es darüber hinaus möglich, Pakete zu empfangen und auszuwerten, die nicht für diesen Netzwerkadapter bestimmt sind. Zusätzlich ermöglicht `tcpdump` die Auswertung von zuvor in Dateien gespeicherten Paketen. Mittels Parametern, die bei Programmstart auf der Kommandozeile angegeben werden müssen, steuert der Benutzer das Verhalten von `tcpdump` und übergibt Filter an das Programm, nach denen die Pakete ausgewertet werden sollen. Haupteinsatzgebiete von `tcpdump` sind:

- Fehlersuche in Programmen, die über das Netzwerk kommunizieren.
- Fehlersuche im Netzwerkaufbau selbst.
- Aufzeichnung und Darstellung der Kommunikation anderer Benutzer und Computer. Benutzern, die Zugriff auf Router oder Gateways innerhalb eines Netzwerkes haben, wird es hiermit ermöglicht, die Kommunikation zwischen verschiedenen Teilnehmern des Netzwerkes zu überwachen und mitzuschneiden. Da einige Protokolle ihre Übertragung unverschlüsselt abwickeln, ist es auf diese Weise möglich, Passwörter und Benutzerdaten aus dem Netzwerk zu erhalten.

The Sleuth Kit

The Sleuth Kit ist eine Sammlung von Befehlszeilentools und einer C-Bibliothek. Damit können Sie Disk-Images analysieren und Dateien daraus wiederherstellen. Es wird hinter den Kulissen von Autopsy und vielen anderen Open-Source- und kommerziellen Forensik-Tools verwendet. Einige der Werkzeuge wurden hier bereits erklärt.

truss

Truss wird mit einem zusätzlichen ausführbaren Befehlszeilenargument aufgerufen und ermöglicht es, die von diesem Argument getätigten Systemaufrufe und die empfangenen Signale auszudrucken.

Volatility

Das Volatility Framework ist eine vollständig offene Sammlung von in Python implementierten Tools für die

Extraktion von digitalen Artefakten aus flüchtigen Speicherproben (RAM). Die Extraktionstechniken werden völlig unabhängig vom untersuchten System durchgeführt und bieten Einblick in dessen Laufzeitzustand.
des Systems. Das Framework soll eine Einführung in die Techniken und die Komplexität geben, die mit der Extraktion digitaler Artefakte aus flüchtigen Speicherproben verbunden sind, und eine Plattform für weitere Arbeiten auf diesem Gebiet bieten.

Wireshark

Wireshark (von englisch wire „Draht“, „Kabel“ und shark „Hai“) ist eine freie Software zur Analyse und grafischen Aufbereitung von Datenprotokollen. Solche Datenprotokolle werden von Computern auf verschiedensten Kommunikationsmedien wie dem lokalen Netzwerk, Bluetooth oder USB verwendet. Das Netzwerk-Analyse-Tool kann Administratoren, Netzwerkexperten und Sicherheitsexperten bei der Suche nach Netzwerkproblemen, der Ermittlung von Botnet-Verbindungen oder beim Netzwerk-Management behilflich sein. Wireshark zeigt bei einer Aufnahme sowohl den Protokoll-Kopf als auch die übertragenen Nutzdaten an. Bei der grafischen Aufbereitung stützt sich das Programm auf die Ausgabe kleiner Unterprogramme wie pcap oder usbpcap, um den Inhalt der Kommunikation auf dem jeweiligen Übertragungsmedium mitzuschneiden.

Scans

Eine der Grundlagen für die Analyse sind unterschiedliche Scan-Methoden. Ein gängiges Tool ist beispielsweise das

Programm chrootkit. Es prüft Dateien nach bekannten Hashwerten, die einem Rootkit entsprechen.

ClamAV als Virenscanner hat keinen direkten Nutzen im Bezug auf ein Linux-basiertes Betriebssystem. Dennoch kann es interessant sein, wenn ein Einbruch ins System stattgefunden hat, das auch von Windows-Clients bedient wird. Beispiele hierfür sind Mailserver oder Webanwendungen, die Inhalte ausliefern. ClamAV prüft dabei Dateien auf auffällige Muster und blockiert je nach Konstellation den Upload der Datei oder informiert den Administrator bei Treffern.

Für die forensische Arbeit ist THOR als Scanner von Interesse. Besonders, da die Lite-Version für Linux-basierte Systeme ausreicht, während die erweiterte Lizenz Windows-spezifische Prüfungen durchführt, die bei Linux-Installationen keinen Mehrwert bieten. THOR führt Basis-Checks durch und ist ein portabler APT-Scanner (Advanced Persistent Threat). THOR benutzt ca. 4.000 YARA-Regeln. Eine YARA-Regel ist eine in C-ähnlicher Textform verfasste Regel, die Schadsoftware anhand der vorgegebenen Signaturen und Bedingungen erkennen und klassifizieren kann. YARA-Regeln lassen sich mit dem kostenlosen YARA-Tool und mit unterschiedlicher Anti-Viren-Software verwenden. Das YARA-Tool ist kommandozeilenbasiert und mit diversen Betriebssystemen nutzbar. Der Scan erkennt Malware oder Schadsoftware basierend auf regulären Ausdrücken.

Dateianalyse

Hinweis: Dokumente wie beispielsweise Sheets können Auffälligkeiten beinhalten. Die Untersuchung der Dateien kann Zeit in Anspruch nehmen.

Für die Dateianalyse muss das Image nicht unbedingt gemountet sein, sondern es kann mit Werkzeugen wie `fls` oder `$ mac-robber` der allozierte Bereich ausgelesen und über Inodes, IDs und weitere Werkzeuge ausgegeben werden. Somit finden lediglich Lesezugriffe statt und die Image-Datei wird nicht verändert.

```
$ fls -f linux-ext2 -m / -r /path/to/image.dd > /path/to/body.fls
```

```
$ fls -f linux-ext2 -m /var -r /path/to/image.dde >> /path/to/body.fls
```

Auch `ils` via Inode kann zur Datenanalyse und zur Bereitstellung von Informationen genutzt werden.

```
$ Ils -f <fs type> -m /path/to/image.dd > /path/to/body.fls
```

Die `body.fls` muss nur noch in ein lesbares Format gebracht werden. Dies kann mit `mactime` getan werden. `$ mactime -b /path/to/body.fls MM/DD/YYYY`.

Das Tool `fls` kann mittels Optionen oder übergebenen Argumenten auch gelöschte Daten anzeigen. `$ fls -rd /path/to/image.dd`.

Wiederherstellung von Dateien

Um Dateien aus einer Imagedatei wiederherzustellen, müssen mit dem Befehl `$ istat` zunächst die Objektgröße und die Blöcke angezeigt werden.

Mit dem Befehl `$ istat /path/to/image.dd block` kann der entsprechende Wert ermittelt werden, der anschließend mit dem Befehl `$ fls -rd` genutzt wird.

Die Wiederherstellung erfolgt dann mit dem Befehl `$ icat`.

`$ icat /path/to/image.dd block (3.13.23) > /dst/inode_23.file`.

Netzwerk-Analyse

Zur Überprüfung von netzwerkspezifischen Informationen sollten die Logdateien von Anwendungen wie SSH-Server, Firewall, Proxy, DHCP- und DNS-Logs, VPN-Logs, Webserver und Mailserver geprüft werden. Auch die Syslog- und die Systemd-Journal-Dateien sind hierzu interessant. Sollten größere Lücken mit fehlenden Informationen entstanden sein, wurden wahrscheinlich Spuren verwischt. Ebenso sind die Netzwerkflows von Interesse, die an eine Netzwerksenke Metadaten senden. Darin kann beobachtet werden, wer wann Pakete welcher Größe versendet hat.

Active Directory

Wenn ein Active Directory für die Benutzerverwaltung genutzt wird, sollten die Aktivitäten geprüft werden, um festzustellen, welcher Benutzer wann Lesezugriffe durchgeführt hat bzw. aus welcher Quelle diese getätigt wurden.

PCAPs

In einer Infrastruktur, in der der Traffic durch eine Paketinspektion überwacht wird, können mittels TLS-Aushebelung und Man-in-the-Middle-Angriffen Informationen der Netzwerkpakete analysiert werden. Dieses Vorgehen ist jedoch sehr aufwendig.

Vorsicht bei der Betrachtung von IPs

Es besteht die Möglichkeit, dass die IP-Adressen gespooft wurden, wodurch Requests mit einer falschen IP-Adresse an eine Infrastruktur gesendet werden. Um solche gespooften IPs zu erkennen, ist die Mitarbeit und Hilfe der ISPs erforderlich. Bei IDS-Mitschnitten kann über die TTL und die Hops geprüft werden, ob der Request von der protokollierten IP stammt.

Spoofing

In den IDS-Informationen kann die Initial-TTL entnommen werden. Diese wird von der vermuteten TTL des Betriebssystems subtrahiert und um eins addiert.

Initial TTL – gelogte TTL + 1 = Hop Count

128 (Windows) – 122 (Log) + 1 = 7.

Mittels eines Traceroutes auf die IP-Adresse kann die Echtheit dieser überprüft werden.

Routen

Mittels Glasses kann geprüft werden, ob die Route auch vorhanden ist. Dafür können wir uns auf den Route-Server von AT&T verbinden.

```
$ telnet route-server.ip.att.net
[...]
route-server > show route <IPv4-Adresse>
```

False Flag

Auch wenn wir wissen, aus welcher Quelle der Angriff stattfand, ist nicht bekannt, ob die Inhaber*innen des Hosts auch den Angriff getätigt haben. Es kann sich auch um einen übernommenen Server einer dritten Person handeln, die unbeteiligt war, oder um einen rotierenden Container bzw. eine VM eines Cloud-Anbieters. Auf dem System können auch Dokumente in kyrillischer Schrift hinterlegt sein, um einen Angriff aus Russland zu suggerieren, während dieser tatsächlich aus Nordkorea, den USA, der Schweiz oder der Troll-Station in der Antarktis durchgeführt wurde.

Hackback ist ein No Go

Übermotivierte Administratoren können gegebenenfalls die Lust verspüren, die erkannten Hosts zurückzuhacken, um sich entweder zu rächen oder Erkenntnisse zu gewinnen. Davon ist grundsätzlich immer abzuraten, da dies mehr Schaden verursacht als Nutzen bringt.

Ein ungesicherter Host könnte hierfür genutzt worden sein, der gekapert und in ein Botnetz hineingezogen oder als Proxy genutzt wurde. So kann dieser Host auch eine kritische Infrastruktur eines Landes sein, die entsprechend geschädigt wird, wodurch wiederum die Wasserversorgung, die Stromversorgung oder die Gesundheitsversorgung beeinträchtigt wird. Beispiele für ungesicherte VNC-Verbindungen können unter https://computernewb.com/vncresolver/browse/ eingesehen werden. Ein Hackback kann somit auch strafrechtlich verfolgt werden, wenn dadurch Menschen zu Schaden kommen.

Ein Hackback verursacht in der Regel nur Kollateralschäden und hat für niemanden einen Nutzen oder Mehrwert.

Quellen:

Angriff durch Systemd Service File (Blog)
https://blog.uberspace.de/2023/11/kompromittierung-von-aquila/

AVML (Repository)
https://github.com/microsoft/avml

BSI Leitfaden IT-Forensik (Buch)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2

Computer Forensik iX Edition - Dpunkt Verlag (Buch)- 3-86490-133-2

Debian Administrator Handbook (Buch)
https://debian-handbook.info/

Einblick in die Forensik (Video):
https://media.ccc.de/v/DS2017-8682-datenspuren_auswerten

Einführung in das Thema Antiforensik (Video):
https://media.ccc.de/v/28c3-4828-de-antiforensik

Einfürhung in die Forensik (Video):
https://media.ccc.de/v/froscon2023-2856-fruher_oder_spater_erwisch_ich_euch_alle#t=1136

ForensicWiki (Dokumentation)

https://forensics.wiki

Honeypot Forensic (Video):
https://media.ccc.de/v/105_Honeypot_Forensics

Kali Linux Handbook (Buch):
https://commons.wikimedia.org/wiki/File:Kali-Linux-Revealed-2021-edition.pdf

Kali Linux Tools (Dokumentation):
https://www.kali.org/tools/

LiME (Repository)
https://github.com/504ensicsLabs/LiME

Menschliche Faktoren der IT-Sicherheit (Video)
https://media.ccc.de/v/36c3-11175-hirne_hacken

Nfdump (Repository)
https://github.com/phaag/nfdump

Nmap (Wikipedia Artikel)
https://de.wikipedia.org/wiki/Nmap

OpSec für Datenreisende (Video)
https://media.ccc.de/v/35c3-9716-du_kannst_alles_hacken_du_darfst_dich_nur_nicht_erwischen_lassen#t=635

Panel zu IT-Security Berufe (Video)
https://media.ccc.de/v/rc3-2021-haecksen-202-it-security-profes

Präsentation Templates zu Security Kursen
https://github.com/kramse/security-courses

Sleuthkit (Dokumentation)
https://wiki.sleuthkit.org

Südwestfalen Incident Response (Bericht)
https://www.sit.nrw/fileadmin/user_upload/SIT_Incident_Response_v1.1.pdf

Tcpdump (Wikipedia Artikel)
https://de.wikipedia.org/wiki/Tcpdump

Über Digitalforensik und ihre Möglichkeiten (Video)
https://media.ccc.de/v/gpn21-186--frher-oder-spter-erwisch-ich-euch-alle-ber-digitalforesnik-und-ihre-mglichkeiten

Universität der Bundeswehr: Forensik (Seminararbeit)
https://www.unibw.de/technische-informatik/mitarbeiter/professoren/dreo/publikationen/seminararbeiten-forensik-2013.pdf

Verhandlung mit Epressern (Video)
https://media.ccc.de/v/37c3-12134-hirne_hacken_hackback_edition

Volatility (Repository)
https://github.com/volatilityfoundation/volatility

Wireshark (Wikipedia Artikel)
https://de.wikipedia.org/wiki/Wireshark

wolfram77web (Repostiroy)
https://github.com/wolfram77web/app-peid