01 | 21 Sonderdruck für Greenbone Networks

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

# Greenbone Security Manager 150

www.it-administrator.de

## Greenbone Security Manager 150

# Ohne Mut zur Lücke

von Dr. Christian Knermann


Quelle: Greenbone Networks

Der deutsche Hersteller Greenbone Networks bietet mit dem Greenbone Security Manager 150 eine Hardware-Appliance an, die kleinen und mittelgroßen Unternehmen beim Schwachstellenmanagement helfen soll. Hierfür unterstützt das Gerät vielfältige Sicherheitsscans und auf Wunsch sogar Testangriffe. IT-Administrator hat das System ausprobiert und war von dessen Funktionsumfang begeistert.

Wer sich auf die Suche nach Produkten für die Netzwerksicherheit begibt, lenkt seinen Blick vermutlich zunächst in Richtung Silicon Valley und denkt nicht unbedingt an Osnabrück. Doch genau dort sitzt mit Greenbone Networks ein Hersteller, der sich bereits seit 2008 ganz Open-Source-basierter Software für das Schwachstellen-Management verschrieben hat.

Mit dem Greenbone Security Manager (GSM) bieten die Sicherheitsexperten dabei ein ganzes Portfolio an physischen [1] und virtuellen [2] Appliances für Unternehmen aller Größenordnungen an. Herzstück der Appliances bildet das hauseigene "Greenbone OS" (GOS) auf Linux-Basis, das den Open Vulnerability Assessment Scanner (OpenVAS [3]) sowie den Greenbone Security Feed integriert.

### OpenVAS als Basis

Bei OpenVAS handelt es sich um einen vollumfänglichen Schwachstellenscanner für authentifiziertes und nicht-authentifiziertes Testen auf Sicherheitslücken. Greenbone Networks ist die treibende Kraft hinter dem Open-Source-Projekt und entwickelt es seit 2009 als freie Software unter der GNU General Public License (GNU GPL) kontinuierlich fort.

Ursprünglich entstand OpenVAS aus vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geförderten Arbeiten als Reaktion darauf, dass die Macher des Schwachstellen-Scanners "Nessus" von einer Open-Source-Lizenz auf ein proprietäres Geschäftsmodell wechselten.

Greenbone stellt dabei heraus, dass es sich bei seinem GSM-Portfolio um komplett überprüfbare Produkte "made in Germany" handelt. Auf Basis eines Lizenzvertrags mit dem BSI ist der GSM bei über 80 Bundesbehörden im Einsatz. Greenbone stellt alle Appliances selbst her und kümmert sich auch um den direkten Support.

OpenVAS bildet zusammen mit weiteren Open-Source-Modulen die technische Basis für das Greenbone Vulnerability Management (GVM), das wiederum die Grundlage für die kommerzielle GSM-Produktfamilie bildet. Einer der wichtigsten Bausteine ist der von Greenbone täglich aktualisierte Feed, der den GSM mit Informationen zu Network Vulnerability Tests (NVTs) versorgt (Bild 1).

Grundlage hierfür bilden neben Meldungen von Security-Communities, Technologie-Partnern und Kundenfeedback die internationalen Standards zur Nummerierung und Klassifizierung von Sicherheitslücken – Common Vulnerabilities and Exposures (CVE), Common Platform Enumeration (CPE), Open Vulnerability and Assessment Language (OVAL) sowie die hierzulande vom CERT-Bund und DFN-CERT herausgegebenen Sicherheits-Advisories.

Die Trial-Version des GSM erhält mit dem Greenbone Community Feed (GCF) nur eine beschränkte Menge an NVTs. Erst die kommerziellen Appliances haben Zugang zum ausgewachsenen Greenbone

### Greenbone Security Manager 150

**Produkt**
Physische Appliance für das Schwachstellenmanagement.

**Hersteller**
Greenbone Networks GmbH
www.greenbone.net/gsm-150

**Preis**
Listenpreis der getesteten Hardware-Appliance GSM 150: 5985 Euro zuzüglich Wartung für ein Jahr (4000 Euro), drei Jahre (9600 Euro) oder fünf Jahre (14.000 Euro). Projektpreise auf Anfrage.

**Systemvoraussetzungen**
Eine Höheneinheit im 19-Zoll-Rack, Einbautiefe 20 cm plus Netzstecker. Serielle Schnittstelle oder HDMI-Monitor und USB-Tastatur zur Erstkonfiguration. Mindestens ein RJ45-Ethernet-Anschluss. Aktueller Browser zur Bedienung des Webfrontends.

**Technische Daten**
www.it-administrator.de/downloads/datenblaetter

Security Feed (GSF) mit Tests auf mehr als 84.000 bekannte Schwachstellen. Nur der GSF enthält NVTs für diverse Enterprise-Produkte, wie etwa Windows-Server-Betriebssysteme und Anwendungsserver, darunter SharePoint und SQL Server, Netzwerkkomponenten von Palo Alto, Cisco, Juniper oder auch Fortinet. Ebenfalls umfasst nur der Greenbone Security Feed diverse Tests auf Sicherheitslücken in Produkten von Oracle, IBM und VMware sowie in industriellen Steuerungen (SCADA).

## Faire Lizenz

Vom Umfang des GSF profitieren sämtliche Lösungen aus dem Hause Greenbone. So bietet der Hersteller mit der Greenbone Managed Service Platform (GSMP) Security-as-a-Service aus der Cloud. Das setzt aber natürlich voraus, dass der Greenbone Scan Cluster (GSC) seine Scanziele öffentlich erreicht oder per VPN Zugang zu internen Ressourcen erhält. Wer die Schwachstellenanalyse lieber im eigenen Hoheitsbereich behalten möchte, findet im Portfolio der physischen und virtuellen Systeme passende Lösungen für nahezu jede Unternehmensgröße, da die verschiedenen Appliances in verteilten Umgebungen in Form eines Master-Sensor-Betriebs zusammenarbeiten können.

Als Besonderheit lizenziert Greenbone seine Produkte nicht nach der absoluten Anzahl zu scannender Endpunkte. Jede Appliance unterstützt grundsätzlich Scans einer unbegrenzten Anzahl von Zielsystemen. Maßgeblich ist stattdessen die Performance pro 24 Stunden. Die tatsächlich realisierbare Menge an Zielen ist abhängig vom Scanmuster und der Anzahl an IP-Adressen, die der GSM pro Tag prüfen soll. Der Hersteller gibt Richtwerte für alle seine Appliances an [2] und hilft im Rahmen eines PoC dabei, das für eine Infrastruktur passende System auszuwählen.

Uns stand im Test eine Appliance vom Typ GSM 150 zur Verfügung, die laut Greenbone bei typischem Scanverhalten bis zu 500 IP-Adressen binnen 24 Stunden scannt und damit für den Einsatz in kleinen bis mittleren Unternehmen konzipiert ist. Darüber sind die physischen Appliances der Typen 400, 450, 600 und 650 angesiedelt, die auf mittlere Unternehmen sowie Zweigstellen abzielen. Ein GSM 650 scannt pro Tag bis zu 10.000 IP-Adressen. Für sehr große Unternehmen komplettieren GSM 5400 und 6500 die Produktfamilie. In der größten Ausbaustufe schafft ein GSM bis zu 80.000 IP-Adressen pro Tag.

Im Bereich der virtuellen Appliances richten sich GSM ONE und MAVEN an Einsteiger [3]. Im Hinblick auf die Performance entspricht die virtuelle Maschine vom Typ GSM CENO am ehesten dem GSM 150. Darüber angesiedelt sind DECA, TERA, PETA und EXA. Virtuell sind damit maximal 18.000 Ziele pro Tag drin, der Enterprise-Bereich ist den physischen Maschinen vorbehalten.

Grundsätzlich ist der gemischte Master-Sensor-Betrieb von physischen und virtuellen Appliances verschiedener Größenordnungen möglich – allerdings mit der Einschränkung, dass der GSM 150 selbst nicht als Master, sondern nur als Sensor für andere Maschinen agieren kann. Die Rolle des Masters ist erst ab GSM 400 aufwärts verfügbar. So wäre es denkbar, eine der größeren Maschinen im internen Netz einer Unternehmenszentrale als Master aufzusetzen und in geografisch oder logisch getrennten Netzbereichen weitere Maschinen als Sensoren zu betreiben.

Neben einem Onlinebetrieb mit dauerhafter Netzwerkverbindung unterstützt Greenbone auch "Airgap"-Sensoren für teilweise oder ganz abgeschottete Netze, etwa im Fall kritischer Infrastrukturen (KRITIS). Dann ließen sich Konfigurations- und Feed-Updates per Datenübertragung per FTP oder gar komplett offline per USB-Stick vom Master zum Sensor befördern.

## Ersteinrichtung per Konsole

Bevor wir den GSM auf die Jagd nach Schwachstellen schicken konnten, mussten wir das Gerät zunächst in unser Netz integrieren. Das gelingt mittels Zugriffs auf die Konsole, wahlweise per serieller Schnittstelle oder per USB-Tastatur und HDMI-Monitor. Greenbone unterstützt die Ersteinrichtung mit einer textbasierten Menüführung. Ausflüge auf die Shell und weitergehende Linux-Kenntnisse sind nicht erforderlich.

Unsere erste Handlung bestand darin, im Bereich "Setup / User" das Passwort für den Konsolen-Admin zu ändern sowie den initialen Admin-Benutzer für das Webfrontend zu aktivieren. Weiterhin widmeten wir uns dem Menüpunkt "Network / Interfaces" und konfigurierten hier das erste Interface zur Verwendung einer statischen IPv4-Adresse. Die Appliance verfügt über drei weitere Interfaces und beherrscht jeweils bis zu acht vLANs. Wichtig waren noch DNS-Einstellungen sowie das globale Gateway, damit der GSM die Adresse "feed.greenbone.net" auflösen und von dort Feed-Updates beziehen konnte.

Im Bereich "Setup / Services / HTTPS" konnten wir unter dem Punkt "Ciphers" festlegen, welche Verschlüsselungsalgo-

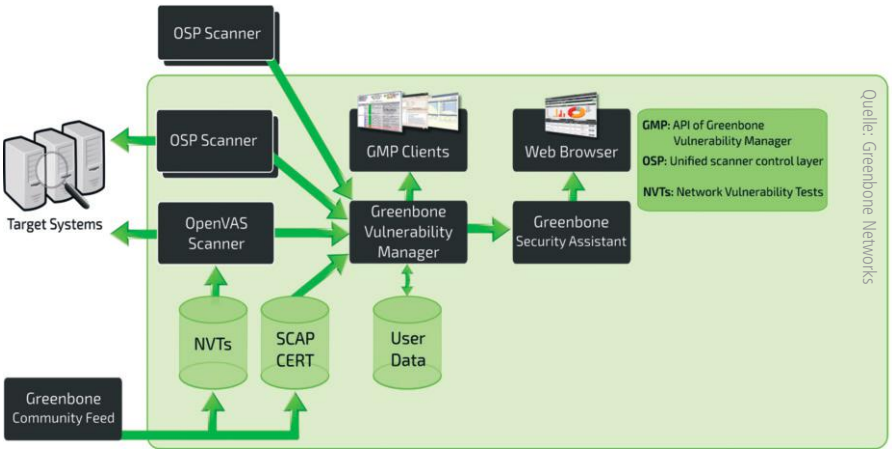


Bild 1: Der Feed versorgt den Greenbone Security Manager tagesaktuell mit Informationen zu neuen Schwachstellen.

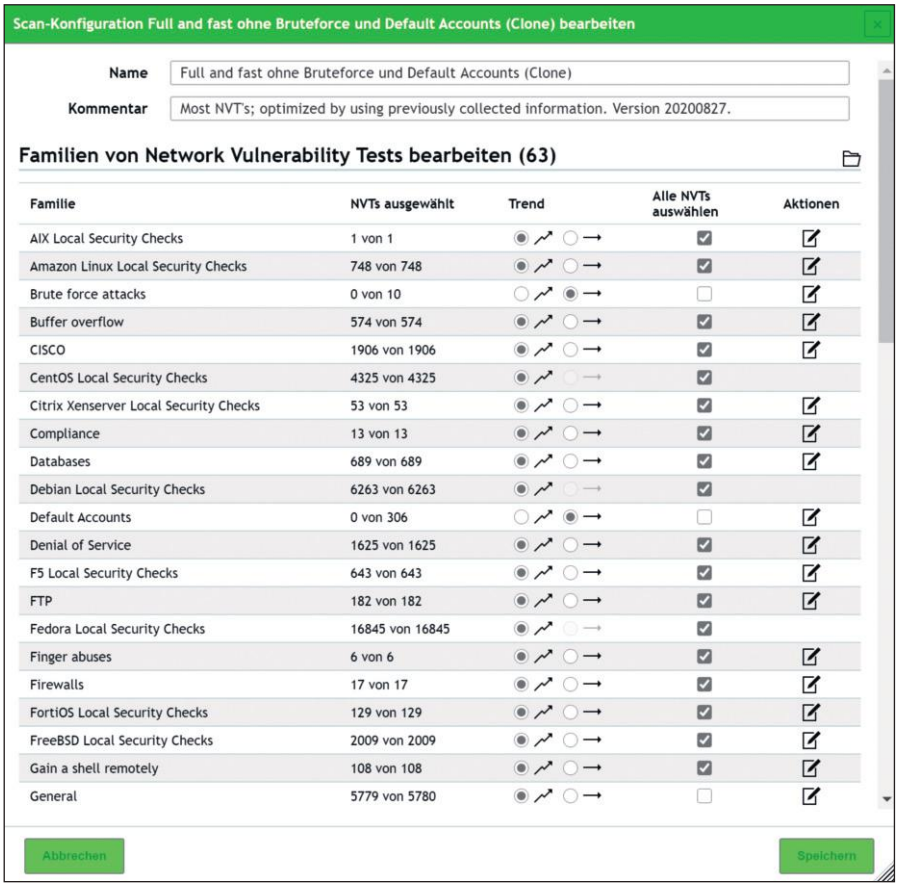


Bild 2: Eine Scankonfiguration kann, unterteilt in 63 Kategorien, mehr als 84.000 Tests auf Schwachstellen beinhalten.

rithmen für HTTPS-Zugriffe zum Einsatz kommen. Der Menüpunkt "Certificate" bot mehrere Optionen zur Verwaltung des Zertifikats. Von Haus aus bringt der GSM ein selbstsigniertes Zertifikat mit. Alternativ bot uns das Setup an, einen CSR zu erzeugen und anschließend ein daraus generiertes Zertifikat unserer eigenen PKI einzuspielen. Für Up- und Downloads startete die Konsole jeweils einen temporären Webserver auf einem separaten Port.

Neben dem interaktiven Zugriff per Webfrontend bot uns die Konsole unter "Setup/ Services / GMP" an, eine Remote-Schnittstelle für das Greenbone Management Protocol zu aktivieren. Es handelt sich dabei um ein API zur Fernbedienung per Kommandozeile. Den SSH-gesicherten Zugriff auf das CLI realisiert ein separater Client zur Installation unter UNIX oder Windows. Dieses GVM-CLI ermöglicht die vollumfängliche Steuerung der Appliance etwa zur Integration mit dem NAC-System von macmon secure. Im Menübereich "Setup / Services / SSH" aktivierten wir noch den SSH-Server des Systems, sodass wir auf die Konsole auch remote zugreifen konnten.

## Feed-Update einmal pro Tag

Die Konsole ist auch die richtige Anlaufstelle, falls der GSM als Sensor einer anderen Appliance oder offline als Airgap-Sensor agieren soll. Als Alternative zum Klassiker Nmap bringt der GSM mit dem Boreas Alive Scanner eine performantere Methode mit, um besonders in großen Netzen schneller aktive Hosts aufzuspüren. In unserer überschaubaren Testumgebung blieben wir jedoch beim voreingestellten Standard.

Unterhalb von "Setup / Mail" konnten wir einen Mailserver mitsamt SMTP-Authentifizierung festlegen, um später aus dem Webfrontend heraus Berichte zu verschicken. Der Bereich "Setup / Remote Syslog" dient der Anbindung an ein SIEM-System. Mittels "Setup Timesync" konfigurierten wir die Zeitsynchronisation per NTP und per "Setup / Time" schließlich den Zeitpunkt, zu dem der GSM täglich Feed-Updates abruft.

Anfänglich aktualisierten wir den Feed über die Aktion "Maintenance / Feed / Update" manuell und hoben das GOS auf die zum Testzeitpunkt aktuelle Version 20.08.5. Weiterhin fanden wir im Menü "Maintenance" die Option für ein Backup des Systems. Das bedeutet beim GSM 150 allerdings die manuelle Sicherung auf ein lokal verbundenes USB-Medium. Automatisierte Backups via SFTP beherrschen erst die Appliances ab GSM 400 aufwärts. Eine weitere Funktion namens "Beaming" migriert das lokale System auf eine andere Appliance. Sobald wir das System mittels "Power / Reboot" neu gestartet und so das Upgrade des Betriebssystems abgeschlossen hatten, konnten wir uns dem Webfrontend zuwenden.

## Umfangreiche Benutzerverwaltung

Das Webfrontend bietet als Einstieg die Seite "Dashboards" mit einer Vielzahl an individuell anpassbaren Diagrammen und Tabellen. Diese informieren übersichtlich über den Status von Scanaufgaben sowie Anzahl und Schweregrad gefundener Sicherheitslücken. Aber das setzt natürlich voraus, dass Scanergebnisse vorliegen. Hierzu mussten wir zunächst noch einige grundlegende Einstellungen vornehmen.

Unsere erste Anlaufstelle im horizontalen Hauptmenü war der Bereich "Administration", unter dem sich neben Diagrammen zu Leistungsdaten des Systems und dem Feed-Status die Verwaltung der Zugriffsrechte fand. Hier konnten wir zur Authentifizierung einen externen LDAP- oder RADIUS-Server anbinden. Dies bedeutet aber nicht, dass der GSM automatisch alle vorhandenen Benutzer aus einem externen Verzeichnisdienst synchronisiert. Wir legten stattdessen gezielt unsere Benutzer im GSM an. Nur deren Authentifizierung erfolgt auf Wunsch statt per lokalem Passwort via LDAP oder RADIUS.

Was genau ein User darf, folgt aus seiner Mitgliedschaft in Rollen und Gruppen. Erstere legen die generellen Berechtigungen zur Verwendung von Befehlen fest.

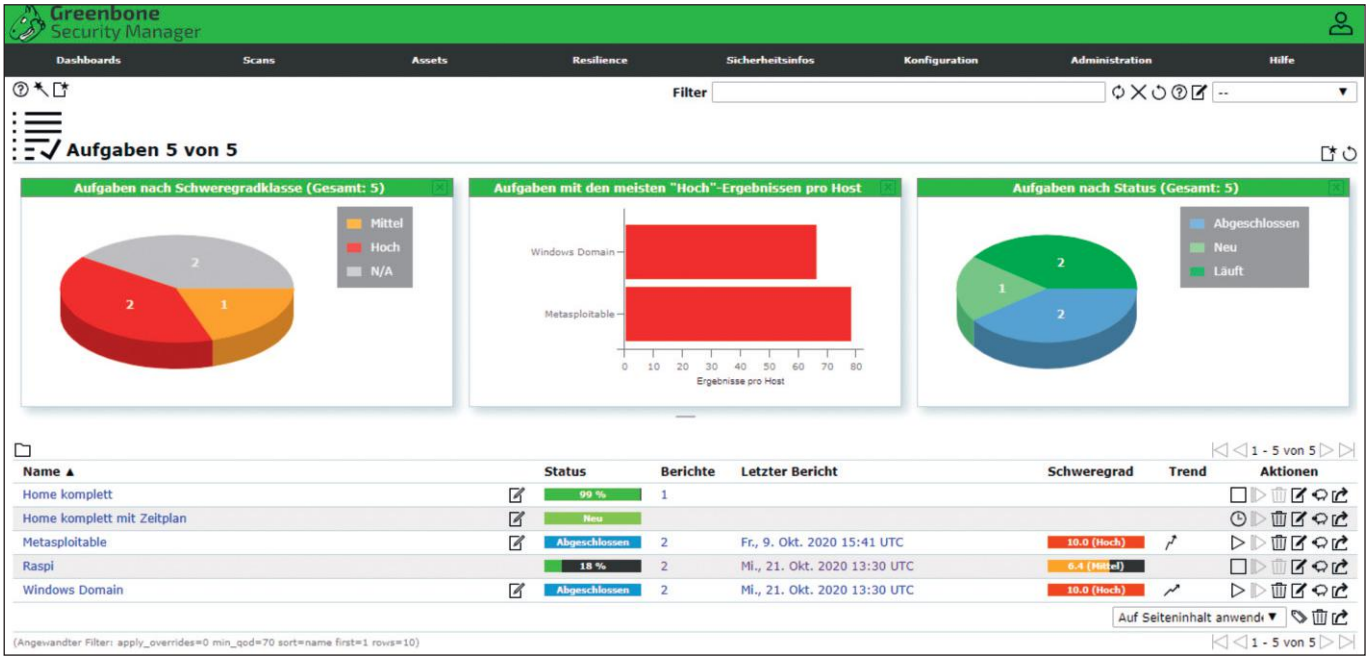


Bild 3: Aufgaben scannen ein oder mehrere Ziele und stellen gefundene Schwachstellen übersichtlich dar.

Einem Least-Privilege-Ansatz folgend reicht für normale Benutzer in der Regel die Rolle "User". Sie umfasst alle nötigen Berechtigungen, abgesehen von der Benutzer-, Rollen- und Gruppenverwaltung. Darüber hinaus haben "Admins" sämtliche Berechtigungen, um das gesamte System zu verwalten.

## Geklonte Rollen

Die vordefinierten Rollen durften wir nicht ändern. Wir konnten diese jedoch klonen, um daraus benutzerdefinierte Rollen zu erzeugen. Die Aktion des Klonens findet sich an diversen Stellen im Webfrontend wieder, der Hersteller verwendet hierfür als Icon die Silhouette eines Schafs – das erste Klonschaf der Geschichte namens Dolly lässt grüßen. Auch Gruppen konnten wir neu erstellen sowie klonen. Nur die Option "Spezielle Gruppen" beim Anlegen einer Gruppe bedarf der Erläuterung: Sie sorgt dafür, dass von einem Mitglied der Gruppe erstellte Ressourcen automatisch auch allen anderen Mitgliedern der Gruppe zur Verfügung stehen. Alternativ dazu kann jeder Benutzer selbst erstellte Ressourcen manuell teilen, was am einfachsten in der Rolle "Admin" gelingt.

Insgesamt ist das Berechtigungskonzept komplex, erschließt sich aber unter Zuhilfenahme des leicht verständlichen Anwenderhandbuchs. Das System zeigt sich damit mandantenfähig und so auch in sehr großen Umgebungen verwendbar. Sind unterschiedliche Teams etwa für Netzwerkkomponenten und Server-Systeme verantwortlich, sieht auf Wunsch jedes Teammitglied nur die Ressourcen in seinem Zuständigkeitsbereich.

## Scans ganzer Netze oder einzelner Hosts

In unserer Testumgebung hatten wir mehrere Zielsysteme vorbereitet, darunter die explizit als angreifbar ausgelegte Linux-Distribution Metasploitable, einen Active-Directory-Domaincontroller unter Windows Server 2019 ohne aktuelle Sicherheitsupdates, weitere Linux-Hosts und einige Clients unter Windows 10 mit unterschiedlichen Patch-Leveln.

Unter dem Punkt "Konfiguration / Ziele" machten wir uns daran, unsere Ziele für Schwachstellenscans einzurichten. Ein Zielobjekt im GSM umfasst einen oder mehrere Hosts oder ganze Netzbereiche. Entsprechend konnten wir im Dialog einzelne IP-Adressen oder ganze Subnetze in CIDR-Notation eintragen, alternativ eine Liste mehrerer Ziele als Datei übergeben. Ebenso durften wir Ausnahmen vom Scan definieren.

Jede Zielkonfiguration umfasst zudem eine Liste der mittels Nmap zu prüfenden Ports. Hier durften wir aus mehreren vorgefertigten Portlisten wählen oder diese unter "Konfiguration / Portlisten" klonen und nach eigenen Wünschen anpassen. Zur Wahl standen hier etwa alle von der Internet Assigned Numbers Authority (IANA) standardisierten TCP-Ports, alle TCP- und UPD-Ports nach IANA, sämtliche TCP-Ports oder auch sämtliche TCP-Ports sowie die "Nmap Top 100" der UPD-Ports.

Im Dropdown-Feld zum Erreichbarkeitstest stand zur Wahl, nach welchem Verfahren Nmap testen soll, ob unter einer bestimmten IP-Adresse ein Zielsystem aktiv ist – ICMP-, ARP-, TCP-ACK- oder TCP-SYN-Ping oder Kombinationen mehrerer dieser Methoden. Optional konnten wir in der Zielkonfiguration auch Anmeldedaten für Linux-, Windows- oder ESXi-Hosts sowie SNMP-Communities mitgeben, vorausgesetzt wir hatten diese zuvor unter "Konfiguration / Anmeldedaten" hinterlegt. Neben Benutzernamen und Passwörtern beherrscht der GSM auch SSH-Schlüssel, Zertifikate und PGP-Verschlüsselungsschlüssel.

## Von passiv bis aggressiv

Ohne Anmeldedaten schaut der GSM mit einer Außensicht auf die Ziele, also aus der Perspektive eines potenziellen Angreifers, der noch keine Zugangsdaten erbeutet hat. Mit Anmeldedaten kann der GSM authentifiziert zugreifen und tiefergehende Erkenntnisse zu Angriffsflächen

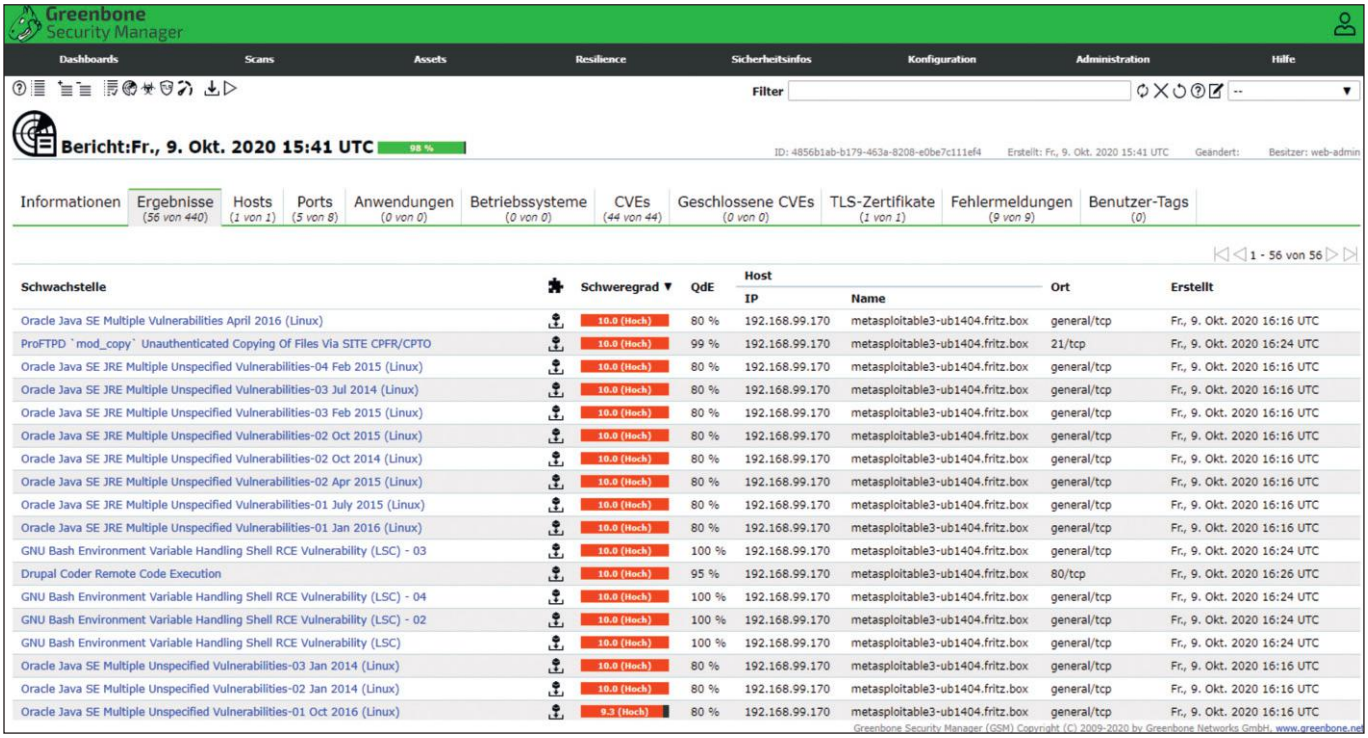


Bild 4: Ein Bericht enthält detaillierte Informationen zu Art und Schweregrad vorhandener Schwachstellen.

gewinnen. Hier entschieden wir uns, zunächst unser komplettes Subnetz ohne Anmeldedaten zu scannen, und legten weitere Ziele für einzelne Hosts mit passenden Anmeldedaten an.

Um einen Scan zu starten, fehlte uns noch eine passende Scankonfiguration. Auch hier brachte der GSM ab Werk unter "Konfiguration / Scan-Konfiguration" diverse Vorlagen von harmlos bis scharf mit. So umfasste die Vorlage "Full and fast" sämtliche Schwachstellen, zum Zeitpunkt unseres Tests 84.481 NVTs, die der Scanner erkennt, ohne sie aktiv auszunutzen. Die schärfste Variante "Full and very deep ultimate" sucht Lücken nicht nur, sondern greift diese auch an. Der Hersteller warnte uns entsprechend, einen solchen Scan nur in einer abgegrenzten Laborumgebung und nie in der Produktion zu verwenden, da er Dienste oder ganze Hosts zum Absturz bringen könnte.

Auch die Vorlage "Full and fast" kann Nebenwirkungen verursachen, da sie verschiedene Brute-Force-Attacken kennt. Systeme mit Schutzfunktionen gegen solche Angriffe könnten sich folglich nach einem Scan sperren und keine Loginversuche mehr zulassen. Der Hersteller empfahl uns entsprechend, die Vorlage "Full and fast" zu klonen und in den Eigenschaften des Klons in der umfangreichen Liste der Familien von NVTs die "Brute force attacks" sowie "Default Accounts" zu deaktivieren.

## Flexible Zeitpläne und Berichte

Weitere Bausteine für Scanaufgaben sind die Benachrichtigungen und Zeitpläne. Beide erwiesen sich als äußerst flexibel konfigurierbar. So können Statusänderungen einer Aufgabe sowie neue oder aktualisierte Schwachstellen Auslöser für eine Benachrichtigung sein. Weiterhin konnten wir eine Benachrichtigung an Bedingungen knüpfen, sodass sie nur auslöst, wenn ein bestimmter Schweregrad erreicht ist oder sich der Schweregrad im Vergleich zu einem früheren Scan ändert. Neben dem Versand eines Berichts per E-Mail bot der GSM diverse weitere Übertragungsmethoden, darunter SCP und SMB sowie Schnittstellen zu den Drittanbieter-Systemen verinice.PRO, TippingPoint SMS und Alemba vFire.

Die Zeitpläne ließen keine Wünsche offen. So konnten wir Scanaufgaben nach Stunden, Tagen, Wochen, Monaten, Jahren oder komplett benutzerdefinierten Bedingungen wiederholen. Dabei übermittelt der GSM die Berichte in verschiedenen Formaten unter anderem als XML, CSV, TXT, PDF oder als HTML, und das mit zielgruppengerecht zugeschnittenen Inhalten. So fanden wir unter "Konfiguration / Berichtsformate" 20 Vorlagen – sehr detaillierte für Sicherheitsbeauftragte ebenso wie auf das Wesentliche konzentrierte für Entscheider.

Alle Optionen konnten wir schließlich unter "Scans / Aufgaben" zu einem Vorgang mit gewünschtem Scanziel, optional Benachrichtigung und Zeitplan, sowie der Scankonfiguration verknüpfen. Dabei durften wir weiterhin wählen, ob der Scan auch gleich alle gefundenen Objekte als Assets erfassen soll. Falls ja, füllt der GSM unter dem Punkt "Assets" im Hauptmenü die Kategorien Hosts, Betriebssysteme und TLS-Zertifikate mit sämtlichen im Netz vorhandenen Objekten und deren Sicherheitsbewertung.

## Alarmierende Ergebnisse

Nachdem wir einige Aufgaben auf dem gesamten Subnetz und einzelnen Hosts ausgeführt hatten, konnten wir unter "Scans / Berichte" die Details einsehen. An dieser Stelle zeigt der GSM zu jeder Aufgabe einen ausführlichen Bericht an, und das unabhängig davon, ob eine Benachrichtigung auch einen Bericht per E-

Mail verschickt. So lieferte unser Scan des Subnetzes ohne Authentifizierung zunächst einige Schwachstellen mit mittlerem Schweregrad, die sich sämtlich durch Konfigurationsänderungen auf den Zielsystemen korrigieren ließen. Dies betraf einen MQTT-Broker, der Zugriffe ohne Anmeldung zuließ, mehrere Webfrontends von Servern und Netzkomponenten, die Informationen per HTTP im Klartext übermittelten, sowie Zertifikate mit zu schwachen Signaturalgorithmen.

Deutlich dramatischer erwies sich die Situation jedoch, sobald wir unsere Linux- und Windows-Systeme mit Authentifizierung analysierten. So zeigte die Metasploitable-VM erwartungsgemäß mit knapp 80 Schwachstellen die größte Angriffsfläche (Bild 3). Aber auch mehr als 60 Schwachstellen auf unserem Domaincontroller wären in einer produktiven Umgebung ein deutliches Alarmsignal.

Der Bericht listete uns auf der Registerkarte der Ergebnisse detailliert auf, um welche Schwachstellen es sich handelte (Bild 4). In den meisten Fällen konnten wir durch die Installation von Updates oder Konfigurationsänderungen reagieren, sodass beim nächsten Lauf der Aufgabe der Bericht weniger kritisch aussah. Und dies ist auch der typische Anwendungsfall für den GSM, nämlich die Aufgaben periodisch zu wiederholen und kontinuierlich mittels Delta-Vergleich zu vorherigen Berichten die gefundenen Schwachstellen zu identifizieren und zu beheben.

Sollte das in Einzelfällen nicht sofort möglich sein, kennt der GSM das Prinzip der Übersteuerungen. Aus Berichten heraus oder unter "Scans / Übersteuerungen" konnten wir einzelne Schwachstellen für das gesamte Netz oder auch nur für bestimmte Hosts dauerhaft oder befristet als Risiko akzeptieren. Sie verschwinden damit zwar nicht komplett aus den Berichten, um nicht den Admin in trügerischer Sicherheit zu wiegen. Wir konnten aber mittels benutzerdefinierter Filter die Übersteuerungen gezielt auf einen Bericht anwenden und so in der Anzeige die Schwachstellen ausblenden, die sich aktuell nicht beheben lassen.

Weitere Perspektiven erschlossen sich uns unter der Ansicht "Scans / Schwachstellen" mit einer Auflistung der gefundenen Lücken über alle bisher gelaufenen Scans sowie mit den Sichten unter "Assets / Hosts" und "Assets / Betriebssysteme", wo wir die Verteilung der Schwachstellen auf einzelne Systeme und Betriebssystem-Gattungen einsehen konnten.

## Audits nach IT-Grundschutz

Zu guter Letzt darf der Menüpunkt "Resilience" mit den Unterpunkten "Compliance Richtlinien", "Compliance Audits" und "Geschäftsprozessanalyse" nicht unerwähnt bleiben. Eine Compliance-Richtlinie ist eine spezielle Scankonfiguration und ein Audit nichts anderes als eine Scanaufgabe, die auf die Einhaltung einer solchen Richtlinie prüft. Auch hier zeigt der GSM seine Orientierung an den Bedürfnissen des heimischen Markts, hilft ein solcher Audit doch dabei, unter anderem die Compliance mit Regelwerken des BSI zu überprüfen.

Ab Werk bringt das System fünf Richtlinien mit, darunter eine zur Überprüfung von TLS-Ports im Hinblick auf die technische Richtlinie TR-03116-4 des BSI zu kryptographischen Vorgaben für Projekte der Bundesregierung sowie eine weitere, die als Klonvorlage für Prüfungen nach den IT-Grundschutz-Katalogen oder dem modernisierten IT-Grundschutz-Kompendium des BSI dient.

Im Bereich der Geschäftsprozessanalyse bot uns der GSM einen grafischen Editor für den Aufbau einer Business Process Map (BPM), mit der wir die Auswirkung einzelner Schwachstellen auf Abläufe im Unternehmen darstellen konnten. Dazu verknüpften wir die an Prozessen beteiligten Systeme. Findet der GSM dann Schwachstellen, weist er hier einfach nachvollziehbar die davon betroffenen Prozesse aus.

## Fazit

Der Greenbone Security Manager erweist sich als praktische Appliance zum umfassenden Aufspüren von Schwachstellen. Die Bedienung erschließt sich nach kurzer Einarbeitung intuitiv, sodass auch Unternehmen ohne hauptamtlichen IT-Sicherheitsbeauftragten schnell zu praktisch verwertbaren Ergebnissen gelangen. Der Umfang des Feeds ist beeindruckend – insbesondere, da das System nicht nur die nach CVE klassifizierten Schwachstellen, sondern auch die Advisories von CERT-Bund und DFN-CERT integriert. Greenbone orientiert sich damit an den Erfordernissen von Unternehmen und Behörden mit hohen Anforderungen an die Sicherheit.

Als besonders fair zeigt sich das Preismodell nach dem Prinzip "Performance pro 24 Stunden". Der GSM 150 untersucht bei typischem Scanmuster 500 Ziele am Tag. Wer nicht täglich die komplette Infrastruktur, sondern unterschiedliche Netzwerkbereiche an unterschiedlichsten Tagen scannt, kann mit der Appliance eine deutlich größere absolute Anzahl an Zielen abdecken. *(dr)* IT

### So urteilt IT-Administrator

| | |
|---|---|
| Umfang des Feeds | 10 |
| Auswertung im Webfrontend | 7 |
| Benachrichtigungen | 8 |
| Mandantenfähigkeit | 7 |
| Lizenzmodell | 8 |

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

### Dieses Produkt eignet sich

**optimal** für kleine und mittlere Unternehmen sowie Behörden, die ihre Infrastruktur systematisch auf Schwachstellen prüfen wollen.

**bedingt** für sehr große Unternehmen. Hier eignet sich der GSM 150 eher als Sensor für eine der größeren Appliances.

**nicht** als Hardware für Unternehmen, die ihre Infrastruktur weitestgehend cloudbasiert betreiben. In diesem Fall erscheint eine der virtuellen Appliances besser geeignet.

### Link-Codes

**[1] Physische Greenbone-Appliances**
l1t12

**[2] Virtuelle Greenbone-Appliances**
l1t13

**[3] OpenVAS**
l1t11