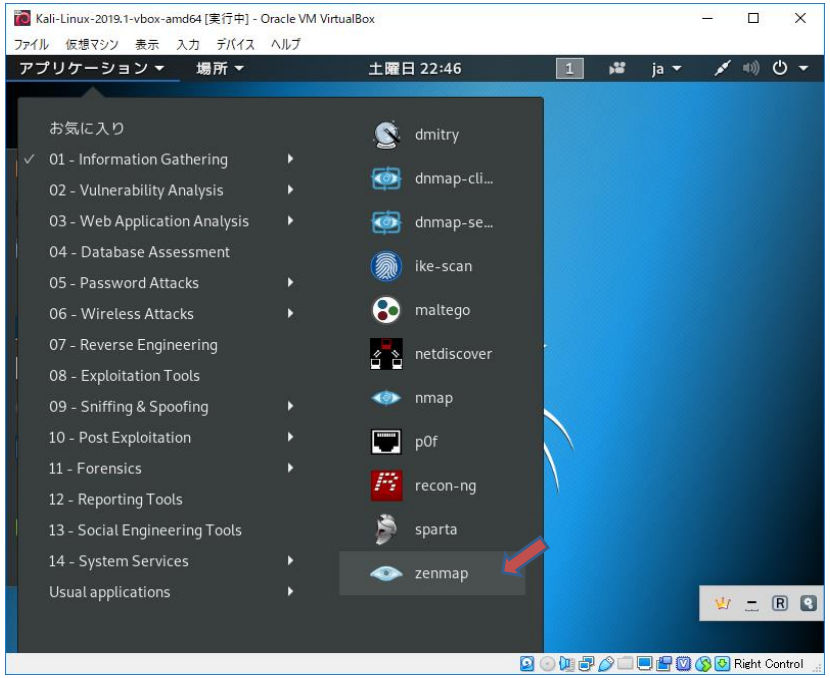
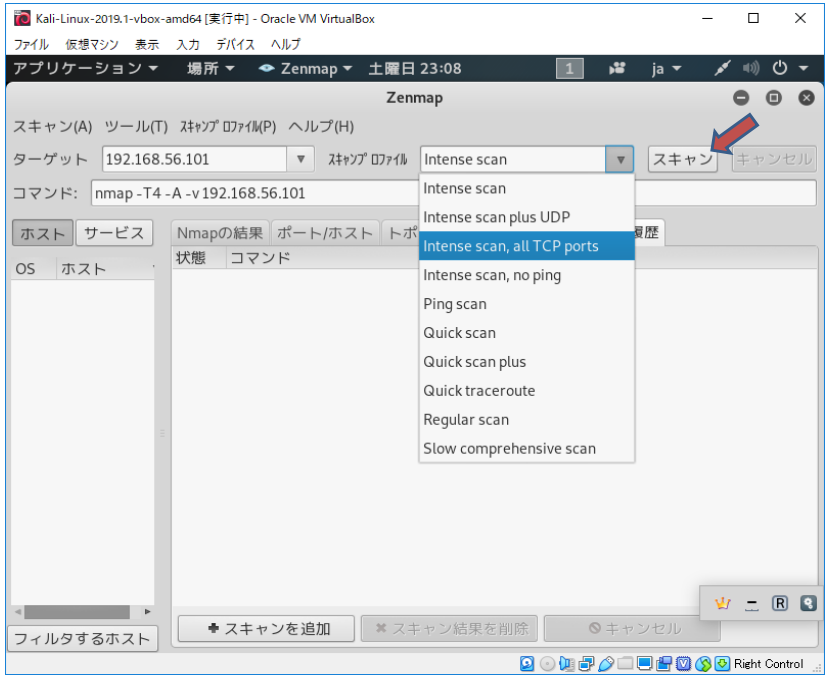
7.4 Nmapによるポートスキャン

NmapのGUIフロントエンドであるZenmapを起動します。

ファイアーウォール越しにポートの開閉状況を確認するには、ファイアーウォールの外部のセグメントからスキャンを掛ける必要がある。
サーバ単体でのポート開閉状況を確認するには、内部のセグメントからスキャンを掛ける必要がある。

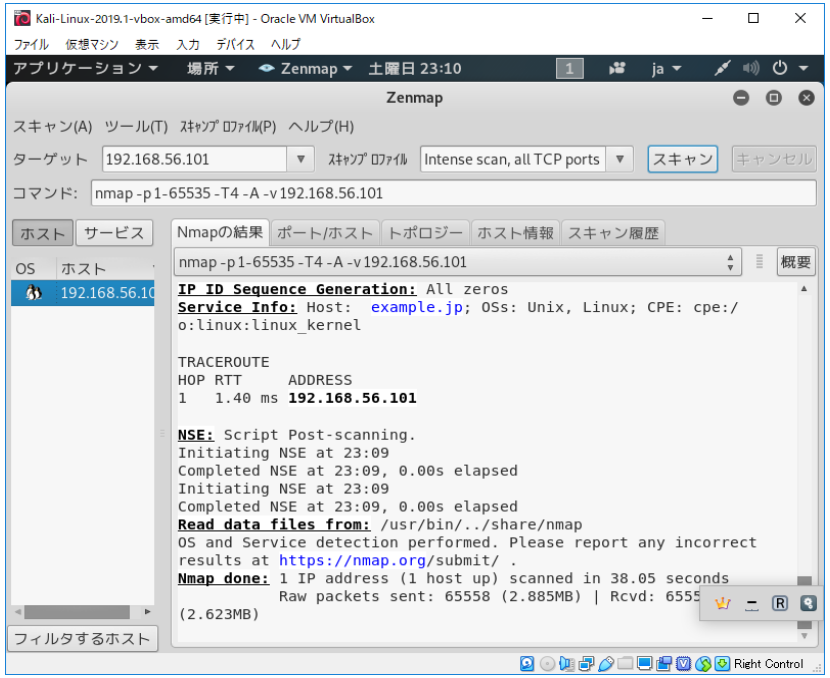
多くのディストリビューション（RHEL,CentOS、Ubuntu,Debianなど）はソフトウエアのバージョンを固定にして、セキュリティパッチを
充てるスタイルなので、見かけのバージョンが古いからといって脆弱性があるとは限りません。
ただし、専門家のセキュリティ診断の結果で、脆弱性判定を受けることがあるのも事実です。



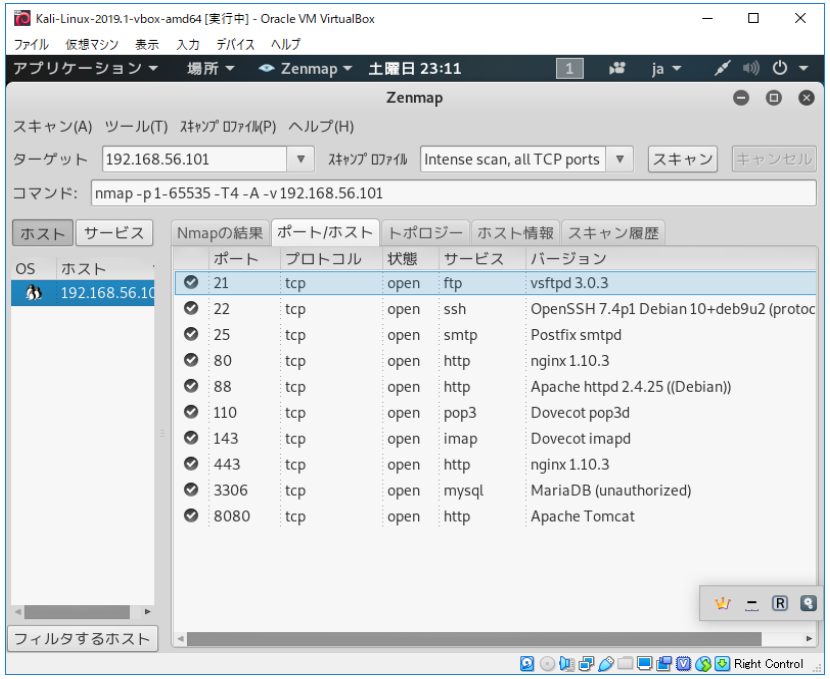


ターゲットに診断するサイトのIPアドレスを入力し、
「Intense scan」→「Intense scan, all TCP ports」を選択し、
「スキャン」をクリック

※ 仮想システム内に名前解決の情報がないので、
IPアドレスを直接指定する。

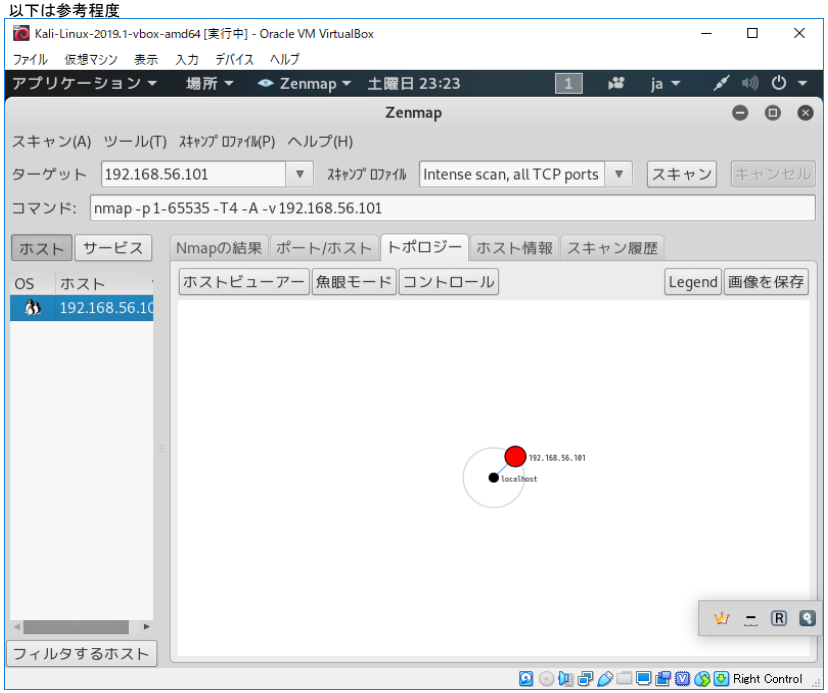


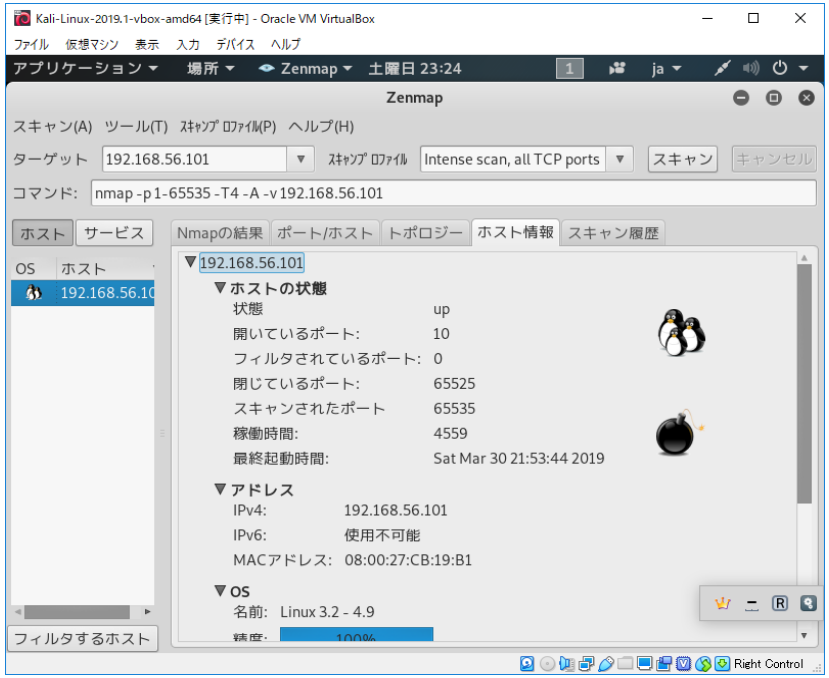
「Nmap done」が表示されたら、スキャンが終了です。

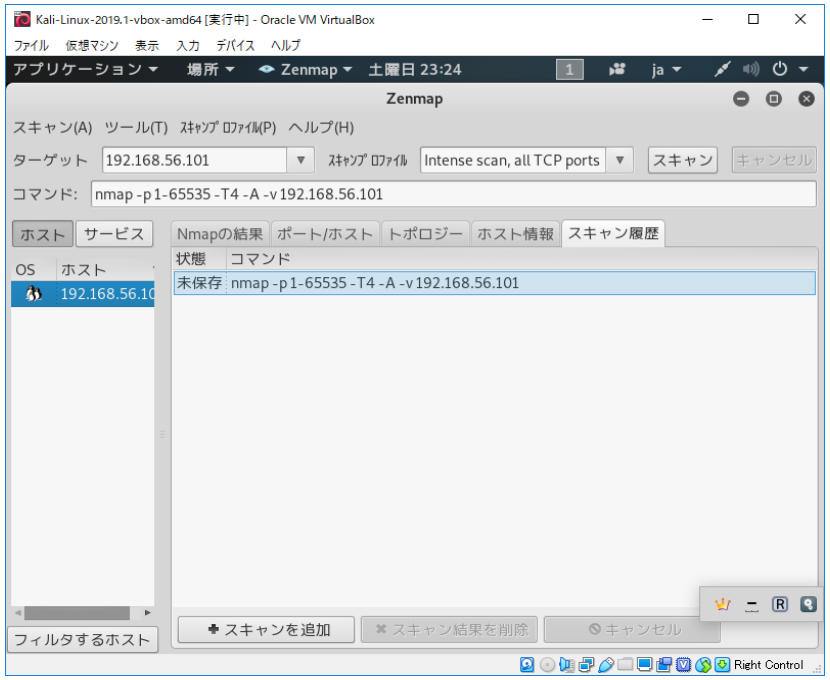


「ポート/ホスト」のタブで、スキャン結果の判断ができます。

以下は参考程度


Kali-Linux-2019.1-vbox-amd64 [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ
アプリケーション 場所 Zenmap 土曜日 23:23
Zenmap
スキャン(A) ツール(T) ｽｷｬﾝﾌﾟﾛﾌｧｲﾙ(P) ヘルプ(H)
ターゲット 192.168.56.101
ｽｷｬﾝﾌﾟﾛﾌｧｲﾙ Intense scan, all TCP ports
スキャン
キャンセル
コマンド: nmap -p 1-65535 -T4 -A -v 192.168.56.101
ホスト
サービス
Nmapの結果
ポート/ホスト
トポロジー
ホスト情報
スキャン履歴
OS
ホスト
192.168.56.10
ホストビューアー
魚眼モード
コントロール
Legend
画像を保存
192.168.56.101
localhost
フィルタするホスト
Right Control


Kali-Linux-2019.1-vbox-amd64 [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ
アプリケーション 場所 Zenmap 土曜日 23:24
Zenmap
スキャン(A) ツール(T) ｽｷｬﾝﾌﾟﾛﾌｧｲﾙ(P) ヘルプ(H)
ターゲット 192.168.56.101
ｽｷｬﾝﾌﾟﾛﾌｧｲﾙ Intense scan, all TCP ports
スキャン
キャンセル
コマンド: nmap -p 1-65535 -T4 -A -v 192.168.56.101
ホスト
サービス
Nmapの結果
ポート/ホスト
トポロジー
ホスト情報
スキャン履歴
OS
ホスト
192.168.56.101
▼192.168.56.101
▼ホストの状態
状態 up
開いているポート: 10
フィルタされているポート: 0
閉じているポート: 65525
スキャンされたポート 65535
稼働時間: 4559
最終起動時間: Sat Mar 30 21:53:44 2019
▼アドレス
IPv4: 192.168.56.101
IPv6: 使用不可能
MACアドレス: 08:00:27:CB:19:B1
▼OS
名前: Linux 3.2 - 4.9
100%
フィルタするホスト
Right Control


Kali-Linux-2019.1-vbox-amd64 [実行中] - Oracle VM VirtualBox
ファイル 仮想マシン 表示 入力 デバイス ヘルプ
アプリケーション 場所 Zenmap 土曜日 23:24 1 ja
Zenmap
スキャン(A) ツール(T) ｽｷｬﾝﾌﾟﾛﾌｧｲﾙ(P) ヘルプ(H)
ターゲット 192.168.56.101 ｽｷｬﾝﾌﾟﾛﾌｧｲﾙ Intense scan, all TCP ports スキャン キャンセル
コマンド: nmap -p 1-65535 -T4 -A -v 192.168.56.101
ホスト サービス
OS ホスト
192.168.56.10
Nmapの結果 ポート/ホスト トポロジー ホスト情報 スキャン履歴
状態 コマンド
未保存 nmap -p 1-65535 -T4 -A -v 192.168.56.101
スキャンを追加 スキャン結果を削除 キャンセル
フィルタするホスト
Right Control