5ZA-03

Linuxディストリビューションを用いた脆弱性調査

氏　名　　岡部　雄太
所　属　　金沢工業大学　工学部　情報工学科

1. 研究の背景と目的

1.1 背景

ソフトウェアの開発に際して．最も懸念すべき事柄としてセキュリティが挙げられる．セキュアかどうかが安全性に直結するが，実際には度々脆弱性が発生, 報告されてしまっている．脆弱性は悪意のある第三者に金銭や重要な情報の不正取得に利用される危険性がある．

1.2 目的

本研究では仮想環境を利用したペネトレーションテスト(以下ペンテスト)を実行し，脆弱性の原因や対策を考察することを目的としている．実際の検証では，フレームワークを用いた攻撃コードの実行に留まらず，攻撃コードを分析しできるだけ手動でその攻撃手法を再現することに着目している．

2. 実験環境

本研究における実験環境では，以下の Linux マシンを利用している．

1. Kali Linux 2019.2

ペンテストやセキュリティ監査を目的とした Linux ディストリビューション．当該マシンのツール「Metasploit framework 5.0」を用いる攻撃者とし，主には攻撃対象の root 奪取を行う．

2. Metasploitable 2

意図して脆弱なバージョンのソフトウェアなどを含んだ仮想マシンであり，これを攻撃対象とする．

3. 検証

3.1 攻撃対象の脆弱性検知

Nmap や Nessus といった脆弱性スキャナを用いて攻撃対象に存在する脆弱性を調査した．Nmap の実行により攻撃対象で開放されているポートやサービス名及びバージョンが判明した．また，Nessus によるスキャン結果では 46 の脆弱性が検知され，この内 9 は Critical 分類であった．

3.2 vsftpd 2.3.4

vsftpd は FTP 接続を待ち受けるデーモンである．Metasploit のコンソール画面で調査すると，vsftpd_234_backdoor を発見した．実行画面に入り攻撃対象の IP アドレスをターゲットに設定し，run で実行するのみで攻撃対象の root 権限を奪取できた．この攻撃コードを分析すると，特定の文字列を含む username が送信されると不要なポートが開放されるという内容であった．telnet により接続を待ち受け，別ターミナルで vsftpd のポート 21 に接続し username を送信した．図 1 に示すようにポート 6200 が開放された．

Fig. 1 telnet connecting to vsftpd

3.3 Apache Tomcat/Coyote JSP engine 1.1

Tomcat の機能には Web アプリケーションマネージャがある．まずは攻撃手法を調査し，ブルートフォース攻撃を実行してアクセスに必要な情報を入手した．次に Bind Shell を Tomcat にデプロイするペイロードを設定し実行すると，root 権限ではないが Tomcat55 権限でシェルを操作で来た．以下の図 2 に奪取したシェルを示す．なお，Web アプリケーションマネージャにアクセスしてプログラムファイルを操作できる．

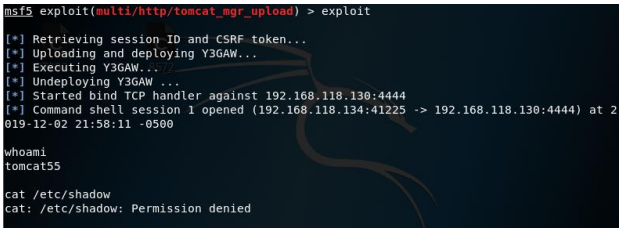

Fig. 2 Tomcat Bind Shell

3.4 Samba 3.0.20

Samba は他 OS で Windows のネットワーク機能を実現するソフトウェアである．Metasploit で Samba 設定ファイルオプションの脆弱性を利用しシェル奪取し，次に Metasploit を用いない侵入手段を探る．攻撃対象の Samba に匿名ログオンし，別ターミナルを nc で接続を待ち受ける．匿名ログオンしているターミナルで，Smbclient の logon で再度ログオンする．その際，echo オプションを付与してシェル本体に受け取った文字列

を渡す．図3に示すように侵入できた．

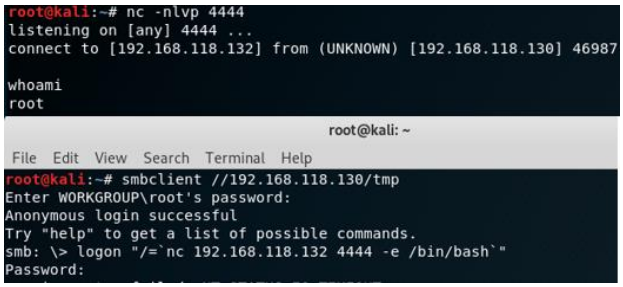

Fig. 3 Samba username map script

3.5 OpenSSL 0.9.8g

Open SSL は暗号通信プロトコルの機能を実装したソフトウェアである．攻撃コードのブルートフォース攻撃により秘密鍵を発見した．図 4 に ssh コマンドによる侵入を示す．

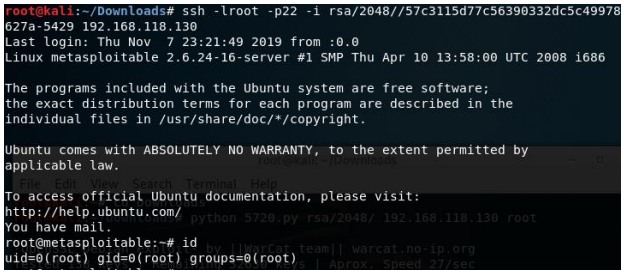

Fig. 4 Illegal Acquisition of RSA

3.6 NFS 1.20

NFS は Linux が動作する PC のディレクトリ共有に用いるファイルシステムである．ssh -keygen で認証用の鍵を作成し，show mount を実行したところ NFS サーバへのアクセス制限がないことが判明した．攻撃者のディレクトリに攻撃対象のルートファイルシステムをマウントさせ，公開鍵を攻撃対象に追加することで図 5 に示すように攻撃対象の root に侵入できた．

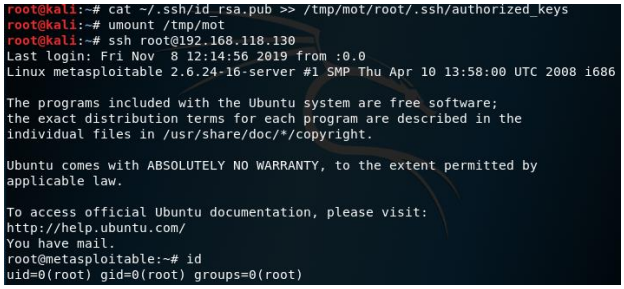

Fig. 5 Attackers can mount an NFS

3.7 UnrealIRCd 3.2.8.1

IRC はクライアント同士のチャットを行うためのソフトウェアである．HexChat を起動し設定を済ませて確認したところ，トロイの木馬を含むバージョンであった．Metasploit でのシェル奪取後 Meterpreter をペイロードに指定した．

3.8 Distcc Daemon 及び udev 117-8 権限昇格

Distcc はコンパイル高速化に用いるプログラムである．Metasploit により一般ユーザで侵入できるので，デバイス管理ツールである udev の脆弱性を利用し権限昇格を行った[1]．まず，別ターミナルで apache2 を起動し攻撃コードをダウンロードできるシンボリックリンクを作成する．次に，udev の攻撃コードを攻撃対象にアップロードし nc で接続を待ち受ける．最後に，一般ユーザのターミナルでシェルへの echo オプションを含む攻撃コードを実行することで図 6 に示すように攻撃対象のマシンを操作することなく権限昇格を実現できた．

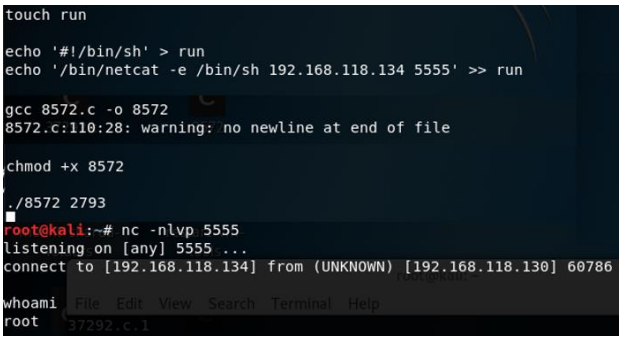

Fig. 6 Local privilege escalation

4. 考察

今回取り上げたソフトウェアにはオープンソースで開発されているものも多い．悪意ある第三者が脆弱性情報の公開後の僅かな時間で攻撃コードを作成されてしまう．

Metasploit にあるようなツールを用いてシステムにペイロードを指定した場合に脆弱であるかどうか反応を調査することが対策の 1 つとして挙げられる．しかし，セキュリティツールなどを用いた対策にも限度がある上，どんなソフトウェアも必ず攻撃を受ける可能性がある．そこで，侵入されてしまうことを前提として侵入後の被害拡大を防ぐことや監視を強化することも重要である．さらには，Web サーバなどの外部公開システムであれば特に迅速な修正パッチの適用が求められる．

参考文献

[1] Sam Bowne：Proj 18x「Privilege Escalation in Metasploitable（平成 29 年 10 月 26 日）」，（https://samsclass.info/124/proj14/p18xLPE.htm，2019 年 11 月 26 日アクセス）．

「Investigating vulnerabilities with Linux distribution」
「Yuta Okabe・Kanazawa Institute of Technology」