ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 8 Issue 4 July 2020

International Manuscript ID : 23482001V8I4007020-198

(Approved and Registered with Govt. of India)

Network Traffic Evaluations Using Python Based Framework for Security and Traffic Fingerprinting

Anil Kumar

Assistant Professor

Department of Computer Science

Govt. College for Women, Hisar, Haryana, India

Abstract

A lot of vulnerabilities are addressed thanks to cyber security experts, who use the latest technologies to their advantage in the network environment. Such concerns include the compromises of privacy, data snooping and theft, integrity, access control, and faked traffic. In addition, false traffic may cause harm to channel capacity. To ensure that people can use technology without being vulnerable, cyber security specialists are working on new ways to implement and integrate higher-level security measures in devices and network infrastructures. More network applications have brought more traffic which has increased security concerns as a way to combat the increase in various kinds of network assaults. Unless it is done properly, chances are high that network or web-based software has vulnerabilities. Traditional administrators have to utilise their own tools to test the network's attacks since the tools are usually only suitable for certain kinds of assaults.

Keywords : Malware Predictions, Network Malware Analytics, Predictive Analytics on Networks

Introduction

Cyber criminals are always striking the hacking community is at an all-time high in an atmosphere with much technology. A lot of techniques and procedures have been developed to defend against such virtual assaults. Still, this domain of securing the applications, devices, networks, computing infrastructure is under research [1].

Broadly, there are two types of attacks in any network based environment

Passive Attacks – In any network environment, when there is the attempt of sniffing the data channels to copy the secret information, it is considered as a passive attack. In this case, the modification of files, directories or credentials is not done. Passive attacks are primarily used to monitor the remote system or server. It is implemented to capture the private information about the system as a spy [2].

Vulnerabilities in Network and Web Applications

It is always desired that the administrators should use different types of penetration and vulnerability testing tools which are meant to assorted attacks. It is done to check the overall deployment on different types of attacks. This methodology ensures that the network or web based environment is secured from multiple attacks without any compromise on security [3].

Penetration Testing and Open Source Tools

Various frameworks and tools are available that provide the ability to do various security audit evaluations, including characteristics like network and web application evaluation. To prevent intruders from ruining their systems, hackers may verify online applications and network devices to look for vulnerabilities that the intruders could use. In the past, network administrators and software developers mostly used penetration testing tools to look for and address any weak-points or vulnerabilities in the network or applications. Penetration testing tests software and hardware to see how they react to simulated assault. During penetration testing, if any application or hardware components behave strangely, appropriate corrective measures and problem solving will be done to deal with the assaults. Penetration testing may be done on everything from devices, websites, servers, and software installations to networks and anything in between.

Several free and open source tools are available for penetration testing and security audits in projects; they may be used for security audits or bug tracking in the deployments [4]. These enormous technologies provide customers the capability to monitor their device's performance while it faces assaults and discover flaws in its security before it is distributed to customers [5].

Python as a High Performance Programming Language for Multiple Applications

As there are many tools and technologies available for penetration testing and security audit, there is need to evaluate the back-end programming which is compatible for network as well as stand-alone environment. It provides multi-functional and high performance features to the penetration testing tool. Python is one of the powerful and cross-platform programming language that is used for most of the high performance environments including cloud computing, big data processing, network programming, socket analytics, data science, statistical analysis and many others. Python provides a huge set of tools which are developed specifically for penetration testing and security audit [6].

Following are the penetration testing and security audio tools developed with Python Programming and these are used widely by the corporate as well as individual usage. These tools are used for digital forensic and vulnerability analysis on different types of hardware and software.

Table 1 : Key Tools for Network Analysis

Dirtbags py-pcap	http://dirtbags.net/py-pcap.html
dpkt	https://github.com/kbandla/dpkt
flowgrep	http://monkey.org/~jose/software/flowgrep/
Habu	https://github.com/portantier/habu
Impacket	http://oss.coresecurity.com/projects/impacket.html
Knock Subdomain Scan	https://github.com/guelfoweb/knock
libdnet	http://code.google.com/p/libdnet/
Mallory	https://bitbucket.org/IntrepidusGroup/mallory
Pytbull	http://pytbull.sourceforge.net/
pypcap, Pcapy and pylibpcap	http://code.google.com/p/pypcap/
pynids	http://jon.oberheide.org/pynids/
Scapy	http://secdev.org/projects/scapy
SubBrute	https://github.com/TheRook/subbrute
Spoodle	https://github.com/vjex/spoodle
SMBMap	https://github.com/ShawnDEvans/smbmap

HULK Based DDoS

Whenever there is DDoS attack on a website, it is known as HULK (HTTP Unbearable Load King) Attack. In HULK attack, the unbearable load is created at HTTP service. By this implementation, a number of virtual connections are created and then fired on the website. If HULK attack is implemented, the particular website gets huge number of connections by fake traffic and then website gets hanged. That’s why HULK is under the umbrella of DDoS attacks to restrict the legitimate users in getting the services. HULK attacks are generally implemented using the scripts of Python, PHP, Java or Perl. Such scripts are easily available on assorted web based repositories of source code [7].

Table 2 : Reverse Engineering and Debugging

Androguard	https://github.com/androguard/androguard
CHIPSEC	https://github.com/chipsec/chipsec
Capstone	http://www.capstone-engine.org/
Frida	http://www.frida.re/
IDAPython	https://github.com/idapython/src
Immunity Debugger	http://debugger.immunityinc.com/
Keystone	http://www.keystone-engine.org/
Paimei	https://github.com/OpenRCE/paimei
PyBFD	https://github.com/Groundworkstech/pybfd/
PyDbgEng	http://pydbgeng.sourceforge.net/
PyEMU	http://code.google.com/p/pyemu/
diStorm	http://www.ragestorm.net/distorm/
mona.py	https://www.corelan.be/index.php/2011/07/14/mona-py-the-manual/
Pefile	https://github.com/erocarrera/pefile
Pydasm	http://code.google.com/p/libdasm/source/browse/trunk/pydasm/pydasm.c
python-ptrace	http://python-ptrace.readthedocs.org/
Uhooker	http://oss.coresecurity.com/projects/uhooker.htm
vdb vtrace	http://code.google.com/p/vdebug/

PytheM Penetration Testing Framework

URL : https://github.com/m4n3dw0lf/pythem

A huge set of software tools and libraries exist written in Python Programming for simulation of different types of attacks. Python is rich in the additional plugins and modules which can be attached for high performance forensic applications and cyber security. PytheM is one of the powerful tools with Python at back-end programming. PytheM provides functions to test the network and web applications with testing of different types of attacks before actual deployment [8].

PytheM is a free and open source penetration testing framework with multi-functional features to analyze the network and web deployment on multiple attacks. It assists the security professionals and administrators to evaluate and perform the security audit of their infrastructure [9].

Downloading and Installation Instructions

PytheM can be installed without any complexity issues on Linux / GNU Platform. PytheM can be installed and executed on Docker containers.

```
[ pythem - Penetration Testing Framework ]
```

Figure 1 : PytheM Penetration Testing Framework

Installation on Ubuntu Linux Distribution

```
$ sudo apt-get update
$ sudo apt-get install -y build-essential python-dev python-pip tcpdump python-capstone libnetfilter-queue-dev libffi-dev libssl-dev
```

Installation using pip:

```
$ sudo pip install pythem
```

Installation of PytheM using source from git repository

```
$ git clone https://github.com/m4n3dw0lf/pythem
$ cd pythem
$ sudo python setup.py install
```

Installation in integration of source and pip:

```
$ git clone https://github.com/m4n3dw0lf/pythem
$ cd pythem
$ sudo python setup.py sdist
$ sudo pip install dist/*
```

Execution and Running of PytheM (With privileges of root)

```
$ sudo pythem
```

On Docker

```
docker run -it --net=host --rm --name pythem m4n3dw0lf/pythem
```

Analysis of different attacks using PytheM

Network administrators may prevent most network attack types if they do regular testing. Network and site administrators should assess their environment in response to a cracked password, and therefore find a secure approach.

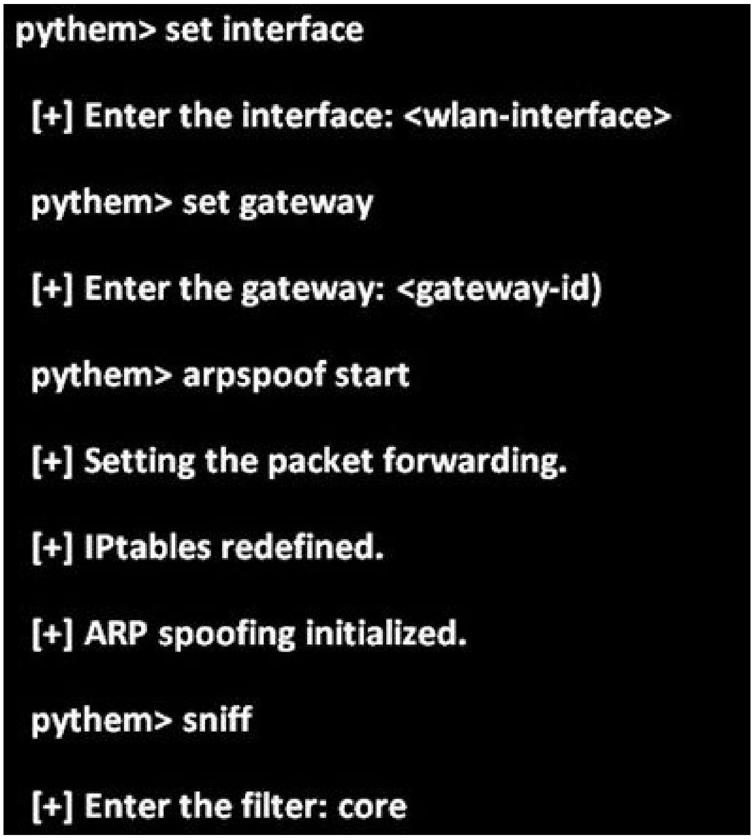
The PytheM toolkit enables users to launch many kinds of network penetration assaults. The information will help security experts anticipate their network's weaknesses [10].

Following are few of the attacks which can be simulated using PytheM

- Man-in-the-Middle Attack
- ARP Spoofing
- DHCP Spoofing
- Brute Force Attacks
- ACK Injection
- PCAP Analysis
- URL Buster
- Overthrow DNS
- Redirections
    - and many others

Implementation of ARP-Spoofing

In ARP Spoofing attack, the malicious or attack source sends the fake or manipulated ARP (Address Resolution Protocol) messages in the network. This process disguises the router and servers which can further steal the information from a privacy aware network environment [9].

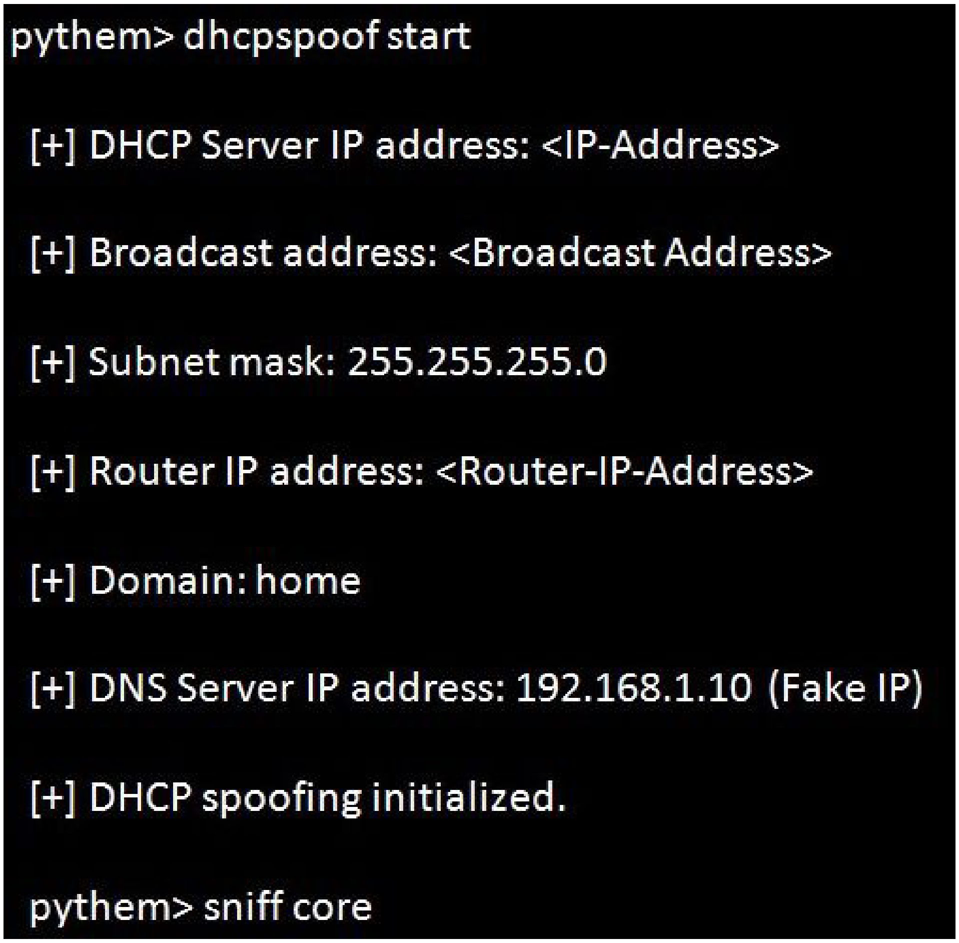


```
pythem> set interface

 [+] Enter the interface: <wlan-interface>

 pythem> set gateway

 [+] Enter the gateway: <gateway-id)

 pythem> arpspoof start

 [+] Setting the packet forwarding.

 [+] IPtables redefined.

 [+] ARP spoofing initialized.

 pythem> sniff

 [+] Enter the filter: core
```

Figure 2 : Penetration Testing using ARP Spoofing in PytheM

DHCP Spoofing Attack or ACK Injection

In DHCP spoofing and starvation attack, the hacker or malicious source can gain access to the DHCP server. By this attack, the attacker can overload the server or important information can be fetched out [10].



```
pythem> dhcpspoof start

 [+] DHCP Server IP address: <IP-Address>

 [+] Broadcast address: <Broadcast Address>

 [+] Subnet mask: 255.255.255.0

 [+] Router IP address: <Router-IP-Address>

 [+] Domain: home

 [+] DNS Server IP address: 192.168.1.10 (Fake IP)

 [+] DHCP spoofing initialized.

 pythem> sniff core
```

Figure 3 : Penetration Testing using DHCP Spoofing and Starvation in PytheM

Conclusion

According to Quick Heal's Annual Threat Report 2019, India's major cities such as Delhi, Bangalore, Mumbai, and Kolkata have been most impacted by cyber attacks, among others. According to the statistics, last year there were over 950 million assault occurrences. A separate article published by Inc42 (a reputable information service) reports that India ranks second in terms of cyber attack prevalence, according to the recently published information security governance market research. The study estimates that cyber attacks cost Indian organisations about 4,552 Rupees per impacted record. Over 50% of the income of 5 million dollars in 2018 was compromised by cyber assaults. These numbers are horrifying, and cyber security and digital forensics must be known to everyone. And in terms of IoT, in which millions of smart devices are linked to each other including smart watches, cameras, and other kinds of e-health gadgets, they, too, are vulnerable to cyber assaults. According to Economic Times, 22% increase in cyber assaults have occurred in IoT installations in India. Research has shown that over 2500 types of malware impacted IoT environments and deployments. A cybersecurity standard is to run software and network hardware in a sandbox prior to deployment to avoid hacking or cyber attacks. Security audits are an efficient means of getting a handle on whether all network assets are protected. Penetration testing in conjunction with tools like PytheM (and related libraries) is the best way to identify all vulnerabilities in the environment.

References

[1] Bekerman, D., Shapira, B., Rokach, L., & Bar, A. (2015, September). Unknown malware detection using network traffic classification. In 2015 IEEE Conference on Communications and Network Security (CNS) (pp. 134-142). IEEE.

[2] Saeed, I. A., Selamat, A., & Abuagoub, A. M. (2013). A survey on malware and malware detection systems. International Journal of Computer Applications, 67(16).

[3] Saxe, J., & Berlin, K. (2015, October). Deep neural network based malware detection using two dimensional binary program features. In 2015 10th International Conference on Malicious and Unwanted Software (MALWARE) (pp. 11-20). IEEE.

[4] Tenenboim-Chekina, L., Barad, O., Shabtai, A., Mimran, D., Rokach, L., Shapira, B., & Elovici, Y. (2013, April). Detecting application update attack on mobile devices through network featur. In 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 91-92). IEEE.

[5] Willems, C., Holz, T., & Freiling, F. (2007). Toward automated dynamic malware analysis using cwsandbox. IEEE Security & Privacy, 5(2), 32-39.

[6] Gandotra, E., Bansal, D., & Sofat, S. (2014). Malware analysis and classification: A survey. Journal of Information Security, 5(02), 56.

[7] Perdisci, R., Lee, W., & Feamster, N. (2010, April). Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces. In NSDI (Vol. 10, p. 14).

[8] Santos, I., Brezo, F., Nieves, J., Penya, Y. K., Sanz, B., Laorden, C., & Bringas, P. G. (2010, February). Idea: Opcode-sequence-based malware detection. In International Symposium on Engineering Secure Software and Systems (pp. 35-43). Springer, Berlin, Heidelberg.

[9] Morales, J. A., Al-Bataineh, A., Xu, S., & Sandhu, R. (2010, September). Analyzing and exploiting network behaviors of malware. In International conference on security and privacy in communication systems (pp. 20-34). Springer, Berlin, Heidelberg.

[10] Burguera, I., Zurutuza, U., & Nadjm-Tehrani, S. (2011, October). Crowdroid: behavior-based malware detection system for android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 15-26). ACM.