Penetrations & Remediations

MIKE HARRIS

556 Forensics

Answers through intelligence

Thanks:

David & Heather Willson
Software Freedom School (sofree.us)
DENHAC (denhac.org)

556 Forensics
Answers through intelligence

Who am I:

Mike Harris
Owner 556 Forensics, LLC.

Experience in system administration (pri. Linux)
Experience in network administration (pri. Cisco)

MIKEDAWG@GMAIL.COM
HTTP://WWW.556FORENSICS.COM/
HTTPS://WWW.LINKEDIN.COM/IN/LINUXMIKEHARRIS

556 Forensics
Answers through intelligence

What am I doing:

Standing up SOCs and CSIRTs (Computer Security Incident Response Teams)

556 Forensics

Answers through intelligence

Gamification:

Gamification is the use of game thinking and game design elements (including game mechanics) in non-game contexts. These game mechanics are designed to shape a game's dynamics (e.g., competitive behavior) and emotions (e.g., anticipation) in order to engage players (e.g. users, customers, employees, voters).

HTTPS://EN.WIKIPEDIA.ORG/WIKI/GAMIFICATION

556 Forensics

Answers through intelligence

Why am I doing this?

After spending my career on the defensive side, I always wanted to see what the red team (attacking team) sees.

556 Forensics

Answers through intelligence

Software we're going to use today:

Virtualization Software (VirtualBox, VMWare, or KVM)
Kali Linux
Nmap/ZenMap
Wfuzz
Wget
WireShark

556 Forensics

Answers through intelligence

Continued:

SQLMap

Hydra

556 Forensics

Answers through intelligence

Virtualization:

In computing, **virtualization** refers to the act of creating a virtual (rather than actual) version of something, including (but not limited to) a virtual computer hardware platform, operating system (OS), storage device, orcomputer network resources.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/VIRTUALIZATION

556 Forensics

Answers through intelligence

Kali Linux:

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. Mati Aharoni, Devon Kearns and Raphaël Hertzog are the core developers.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/KALI_LINUX

556 Forensics

Answers through intelligence

Nmap/ZenMap:

Nmap (*Network Mapper*) is a security scanner originally written by Gordon Lyon (also known by his pseudonym *Fyodor Vaskovich*) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/NMAP

556 Forensics

Answers through intelligence

Wfuzz:

Wfuzz is a tool designed for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), bruteforce GET and POST parameters for checking different kind of injections (SQL, XSS, LDAP,etc), bruteforce Forms parameters (User/Password), Fuzzing,etc.

HTTP://WWW.EDGE-SECURITY.COM/WFUZZ.PHP

Wget:

GNU Wget (or just **Wget**, formerly **Geturl**) is a computer program that retrieves content from web servers, and is part of the GNU Project. Its name is derived from *World Wide Web* and *get*. It supports downloading via HTTP, HTTPS, and FTP protocols.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/WGET

556 Forensics

Answers through intelligence

Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named **Ethereal**, the project was renamed Wireshark in May 2006 due to trademark issues.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/WIRESHARK

556 Forensics

Answers through intelligence

sqlmap:

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

HTTP://SQLMAP.ORG/

556 Forensics

Answers through intelligence

THC-Hydra (hydra):

A very fast network logon cracker which support many different services.

HTTPS://WWW.THC.ORG/THC-HYDRA

556 Forensics

Answers through intelligence

Vulnerabilities to be discussed:

SQL Injection
Shellshock
PHP Code Injection
Insecure File Handling
Weak Credentials

556 Forensics

Answers through intelligence

Resources Used:

HTTP://WWW.VULNHUB.COM

HTTP://WWW.RINGZER0TEAM.COM

556 Forensics

Answers through intelligence

SQL Injection:

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/SQL_INJECTION

556 Forensics

Answers through intelligence

Shellshock:

Shellshock, also known as **Bashdoor**, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

HTTPS://EN.WIKIPEDIA.ORG/WIKI/SHELLSHOCK_(SOFTWARE_BUG)

556 Forensics

Answers through intelligence

PHP Code Injection:

Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection is often disastrous (for instance: code injection is used by some computer worms to propagate).

HTTPS://EN.WIKIPEDIA.ORG/WIKI/CODE_INJECTION

556 Forensics

Answers through intelligence

Weak Credentials:

Authentication-based attacks – guessing, cracking, or reusing valid credentials – factored into four of every five breaches in 2012.

HTTP://WWW.SECUREIDNEWS.COM/NEWS-ITEM/WEAK-CREDENTIALS-ENABLING-CYBER-CRIME/

556 Forensics

Answers through intelligence

QUESTIONS?

MIKEDAWG@GMAIL.COM

HTTP://WWW.556FORENSICS.COM/

HTTPS://WWW.LINKEDIN.COM/IN/LINUXMIKEHARRIS

556 Forensics

Answers through intelligence

MIKEDAWG@GMAIL.COM

HTTP://WWW.556FORENSICS.COM/

HTTPS://WWW.LINKEDIN.COM/IN/LINUXMIKEHARRIS

556 Forensics

Answers through intelligence