Some Tools for Computer Security Incident Response Team (CSIRT)

AfNOG 12

30th May 2011 – 10th June 2011

Tanzania

By

Marcus K. G. Adomey

Overview

Some Unix Commands

Some Selected Tools

- ✓ Snort
- ✓ AirSnort
- ✓ hping
- ✓ Nmap
- ✓ Kismet
- ✓ Tcpreplay
- ✓ Aircrak
- ✓ Tripwire
- ✓ Argus
- ✓ Tor
- ✓ Nepenthes
- ✓ Nessus
- ✓ Wireshark
- ✓ LanSpy

Rational for using tools in CSIRT Management

- ✓ Network analysis
- ✓ Log analysis
- ✓ Incident, Vulnerability or Malware Handling
- ✓ Investigation or research

Other side of the coin

- ✓ At times difficult to use
- ✓ Some of the tools may use by attacker for criminal activities

Important language to know for making your own tool.

- ✓ shell script, sed/awk
- ✓ perl, python, ruby

Unix/Linux command line based tools

(some tools are also available for windows)

Basic Unix command line tools

- ✓ ps, df, dd, dmesg, grep, ls, cd, cp, rm, mv, ifconfig whois, dig (nslookup), traceroute, ping, strings, netstat, top (endless…)

Advance Unix command line tools

- ✓ gnupg , ssh, snort, airsnort, hping2, nmap, kismet, netcat(nc), tcpdump, wget,

tcpreplay, aircrack

Powerful tools.

- ✓ Tripwire, Argus, Tor, Nepenthes

Snort

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS).

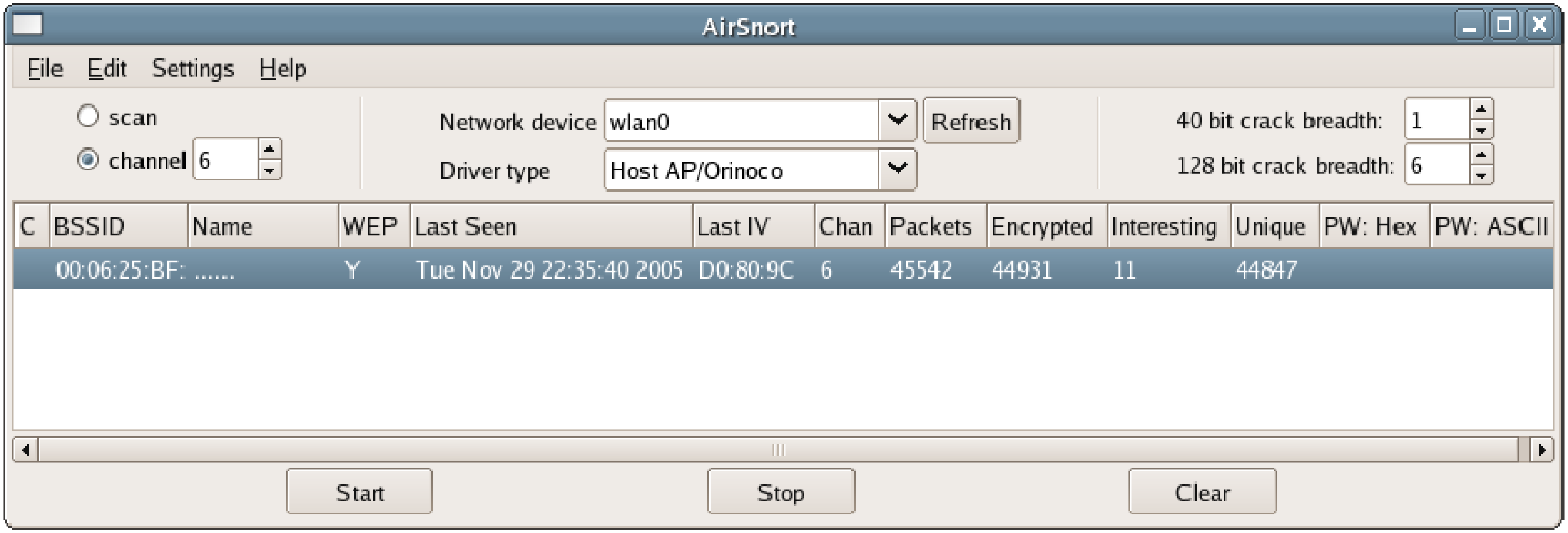
Snort's has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks.

Snort performs protocol analysis, content searching, and content matching.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

AirSnort

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.



○ scan

● channel 6

Network device wlan0

Driver type Host AP/Orinoco

40 bit crack breadth: 1

128 bit crack breadth: 6

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:06:25:BF:	......	Y	Tue Nov 29 22:35:40 2005	D0:80:9C	6	45542	44931	11	44847		

hping

hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique (also invented by the hping author).

The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time.

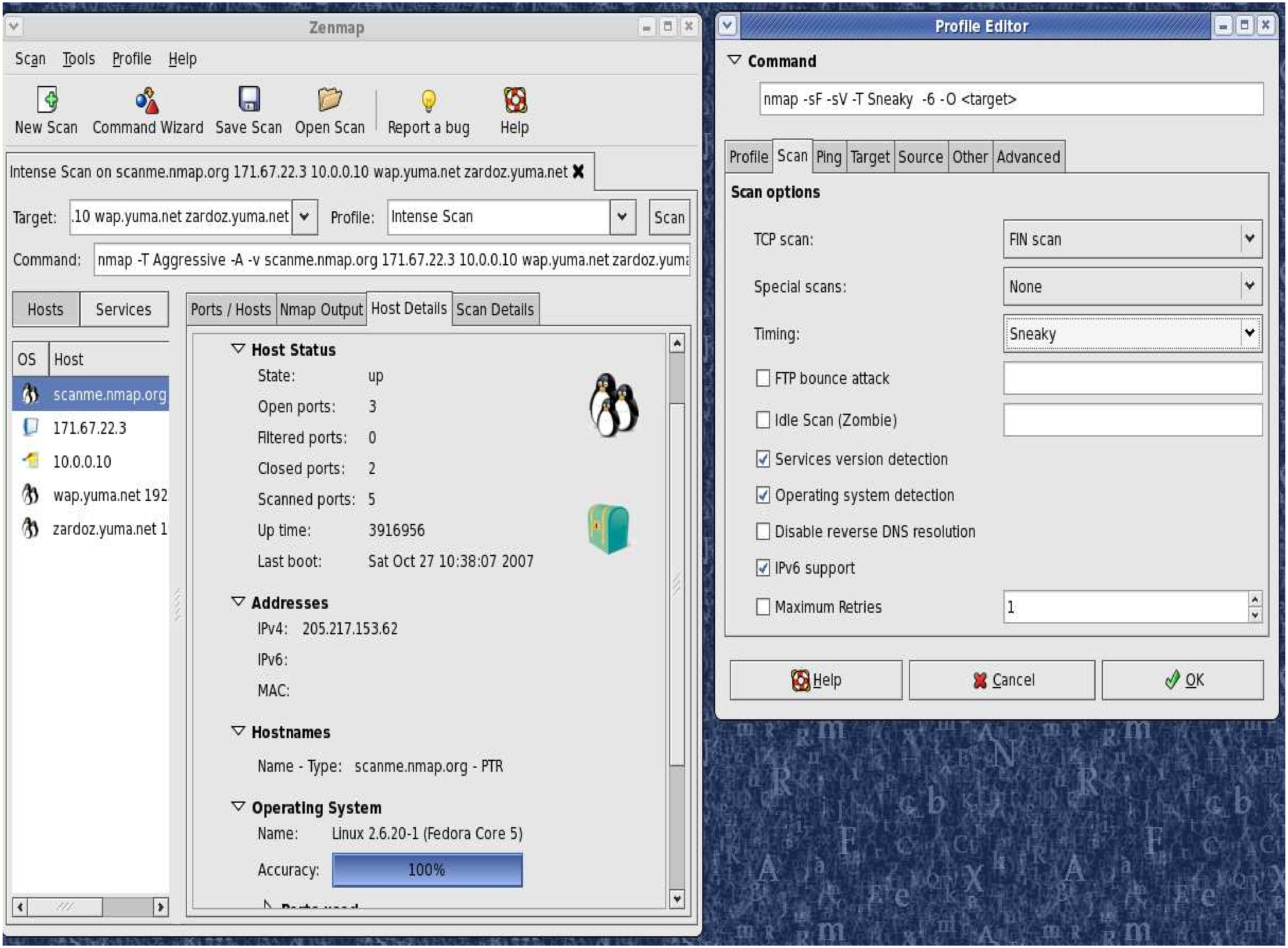
Nmap

Nmap (Network Mapper) is a security scanner 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.

Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run.

Nmap has succeeded to extend its discovery capabilities beyond basic host being up/down or port being open/closed to being able to determine operating system of the target, names and versions of the listening services, estimate uptime, the type of device, presence of the firewall.



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net ✖

Target: .10 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A -v scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yum

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

Host Status

State: up

Open ports: 3

Filtered ports: 0

Closed ports: 2

Scanned ports: 5

Up time: 3916956

Last boot: Sat Oct 27 10:38:07 2007

Addresses

IPv4: 205.217.153.62

IPv6:

MAC:

Hostnames

Name - Type: scanme.nmap.org - PTR

Operating System

Name: Linux 2.6.20-1 (Fedora Core 5)

Accuracy: 100%

Ports used

Command

nmap -sF -sV -T Sneaky -6 -O <target>

Scan options

TCP scan: FIN scan

Special scans: None

Timing: Sneaky

☐ FTP bounce attack

☐ Idle Scan (Zombie)

☑ Services version detection

☑ Operating system detection

☐ Disable reverse DNS resolution

☑ IPv6 support

☐ Maximum Retries 1

Kismet

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins which allow sniffing other media such as DECT.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and infering the presence of nonbeaconing networks via data traffic.

Tcpreplay

Tcpreplay is a suite of BSD GPLv3 licensed tools for UNIX (and Win32 under Cygwin) operating systems which gives you the ability to use previously captured traffic in libpcap format to test a variety of network devices. It allows you to classify traffic as client or server, rewrite Layer 2, 3 and 4 headers and finally replay the traffic back onto the network and through other devices such as switches, routers, firewalls, NIDS and IPS's. Tcpreplay supports both single and dual NIC modes for testing both sniffing and inline devices.

The Tcpreplay suite includes the following tools:

- ✓ ***tcpprep*** - multi-pass pcap file pre-processor which determines packets as client or server and creates cache files used by tcpreplay and tcprewrite
- ✓ ***tcprewrite*** - pcap file editor which rewrites TCP/IP and Layer 2 packet headers
- ✓ ***tcpreplay*** - replays pcap files at arbitrary speeds onto the network
- ✓ ***tcpreplay***-edit - replays & edits pcap files at arbitrary speeds onto the network
- ✓ ***tcpbridge*** - bridge two network segments with the power of tcprewrite
- ✓ ***tcpcapinfo*** - raw pcap file decoder and debugger

Aircrack

Aircrack-ng is a set of tools for auditing wireless networks. It is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

It comprises of:

- ✓ airodump: 802.11 packet capture program
- ✓ aireplay: 802.11 packet injection program
- ✓ aircrack: static WEP and WPA-PSK key cracker
- ✓ airdecap: decrypts WEP/WPA capture files

Tripwire

Tripwire is a free software security and data integrity tool useful for monitoring and alerting on specific file change(s) on a range of systems.

Tripwire functions as a host-based intrusion detection system. It detects changes to file system objects.

When first initialized, Tripwire scans the file system as directed by the administrator and stores information on each file scanned in a database.

At a later date the same files are scanned and the results compared against the stored values in the database. Changes are reported to the user. Cryptographic hashes are employed to detect changes in a file without storing the entire contents of the file in the database.

While useful for detecting intrusions after the event, it can also serve many other purposes, such as integrity assurance, change management, and policy compliance.

Argus

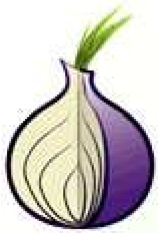
Argus – (Audit Record Generation and Utilization System) is a fixed-model real-time flow monitor designed to track and report on the status and performance of all network transactions seen in a data network traffic stream, doing that by that categorizing IP packets which match the Boolean expression into a protocol-specific network transaction model.

Argus provides a common data format for reporting flow metrics such as connectivity, capacity, demand, loss, delay, and jitter on a per transaction basis. The record format that Argus uses is flexible and extensible, supporting generic flow identifiers and metrics, as well as application/protocol specific information.

Tor

Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. Tor works with many of your existing applications, including web browsers, instant messaging clients, remote login, and other applications based on the TCP protocol.



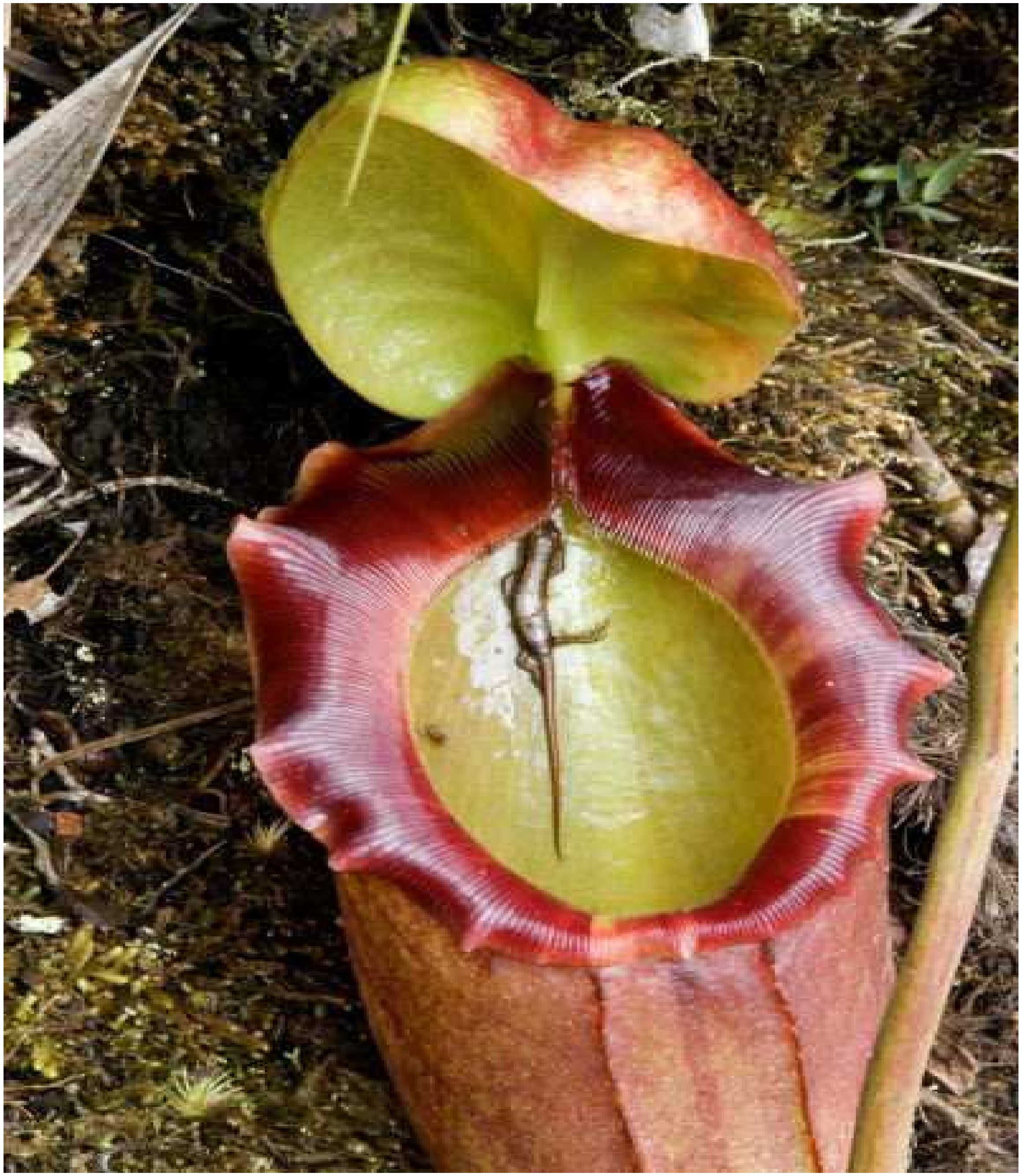
Nepenthes

Nepenthes is a low interaction honeypot to collect information about potential attacks.

Nepenthes is designed to emulate vulnerabilities worms use to spread, and to capture these worms.

There are module interface to:

- ✓ resolve dns asynchronous
- ✓ emulate vulnerabilities
- ✓ download files
- ✓ submit the downloaded files
- ✓ trigger events (sounds abstract and it is abstract but is still quite useful)
- ✓ shellcode handler

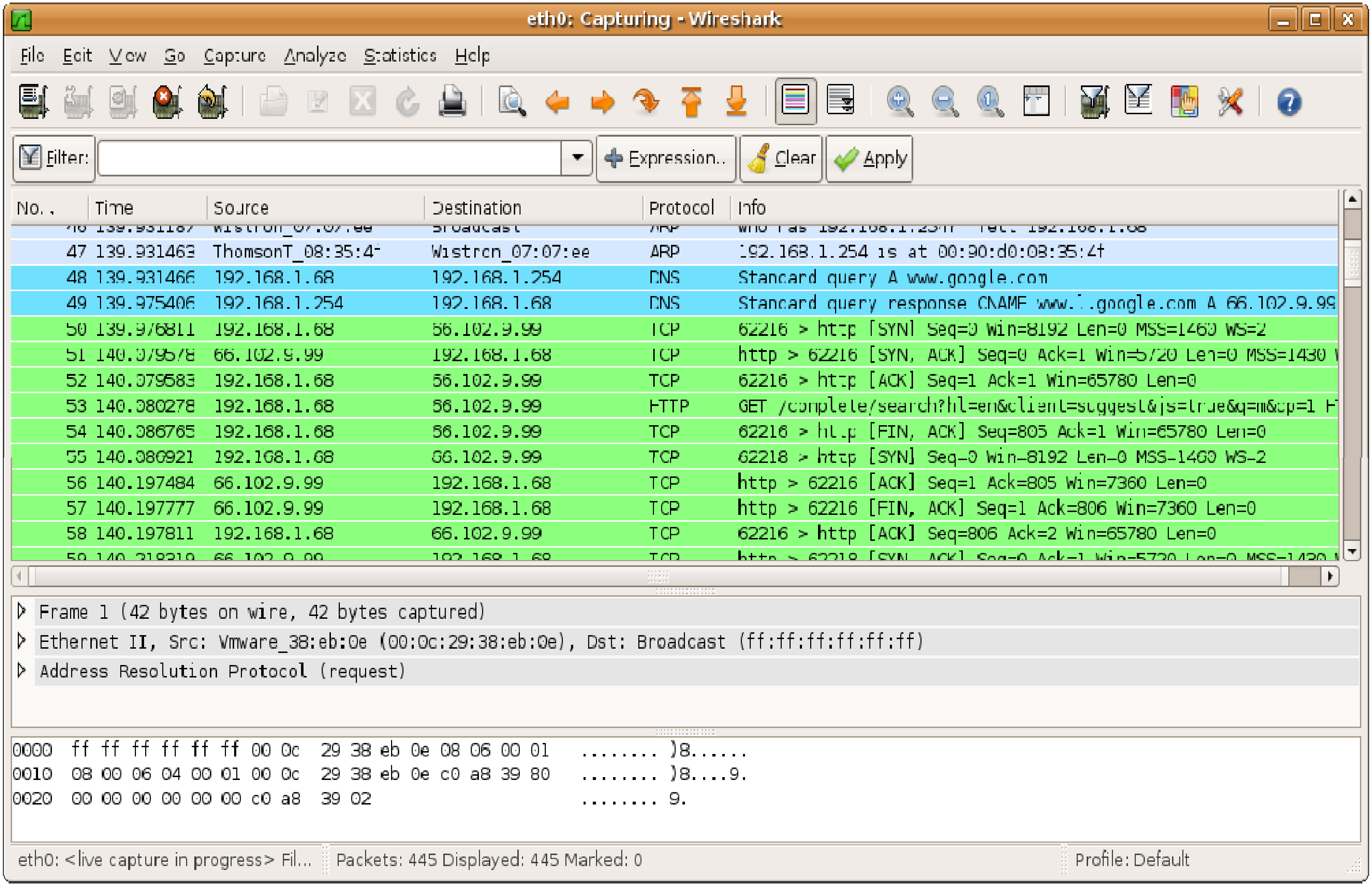


Nessus

The Nessus vulnerability scanner, is the world-leader in active scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks.

Wireshark

Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.



```
No. .  Time        Source              Destination         Protocol  Info
    46 139.931187  Wistron_07:07:ee    Broadcast           ARP       Who has 192.168.1.254?  Tell 192.168.1.68
    47 139.931463  ThomsonT_08:35:4f   Wistron_07:07:ee    ARP       192.168.1.254 is at 00:90:d0:08:35:4f
    48 139.931466  192.168.1.68        192.168.1.254       DNS       Standard query A www.google.com
    49 139.975406  192.168.1.254       192.168.1.68        DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
    50 139.976811  192.168.1.68        66.102.9.99         TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    51 140.079578  66.102.9.99         192.168.1.68        TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
    52 140.079583  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
    53 140.080278  192.168.1.68        66.102.9.99         HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
    54 140.086765  192.168.1.68        66.102.9.99         TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
    55 140.086921  192.168.1.68        66.102.9.99         TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
    56 140.197484  66.102.9.99         192.168.1.68        TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
    57 140.197777  66.102.9.99         192.168.1.68        TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
    58 140.197811  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
    59 140.218219  66.102.9.99         192.168.1.68        TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 W
```

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

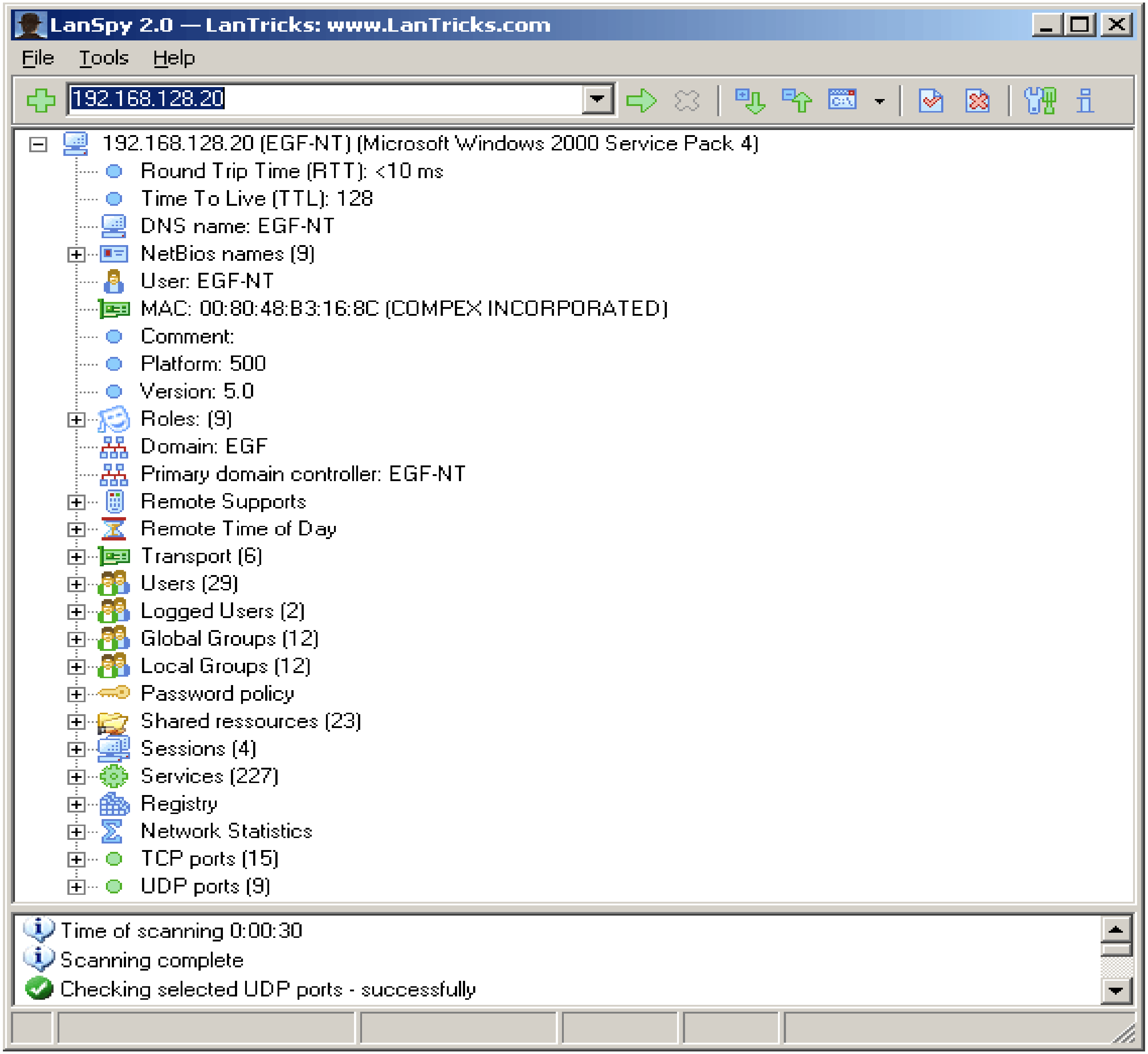
```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

```
eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0   Profile: Default
```

LanSpy

LanSpy is a set of network utilities brought together in a single program with simple and easy-to-use interface. LanSpy help network administrators maintain and manage their networks.

LanSpy includes fast port scanner for gathering information about open ports on remote computer, LanSpy displays services using these ports.



192.168.128.20

```
⊟ 192.168.128.20 (EGF-NT) (Microsoft Windows 2000 Service Pack 4)
     Round Trip Time (RTT): <10 ms
     Time To Live (TTL): 128
     DNS name: EGF-NT
  ⊞ NetBios names (9)
     User: EGF-NT
     MAC: 00:80:48:B3:16:8C (COMPEX INCORPORATED)
     Comment:
     Platform: 500
     Version: 5.0
  ⊞ Roles: (9)
     Domain: EGF
     Primary domain controller: EGF-NT
  ⊞ Remote Supports
  ⊞ Remote Time of Day
  ⊞ Transport (6)
  ⊞ Users (29)
  ⊞ Logged Users (2)
  ⊞ Global Groups (12)
  ⊞ Local Groups (12)
  ⊞ Password policy
  ⊞ Shared ressources (23)
  ⊞ Sessions (4)
  ⊞ Services (227)
  ⊞ Registry
  ⊞ Network Statistics
  ⊞ TCP ports (15)
  ⊞ UDP ports (9)
```

```
Time of scanning 0:00:30
Scanning complete
Checking selected UDP ports - successfully
```