

CSC 300

FINAL REPORT

Hacker Techniques/Tools and Incident
Handling

Ahsan Syed

aksyed2@myseneca.ca

037-553-153

6th August 2017 - Sunday

CSC300 | Final Report

Social Engineering


Social Engineering is a clever hacking strategy that may be used by two types of hackers: the ones that are not very technical or the efficient ones, who like to take shortcuts and get work done ASAP. Overall, I think social engineering is a type of fraud and people should be cautious about it.

Many Social Engineers use common tactics and these are the most common current practices:

- **Phishing:** This is a strategy in which attackers use shortened or embed links that redirect users to suspicious websites in URLs that appear legitimate. This type of attack is usually done to obtain personal information (i.e. usernames, addresses, SIN, contact info). Some phishing emails are poorly crafted but the ones that are crafted in a legitimate fashion are hard to distinguish.
- **Baiting:** This is a strategy where attackers promise an item or good for the information the victim provides. For example, a baiter may offer free downloads to some software, music, or movie if the victim provides their login credentials to a certain website.
- **Pretexting:** This is a strategy in which attackers try to build a credible story that leaves little room for doubt on the part of their target. This method is used to access non-sensitive and sensitive information. For example, an attacker acts like an external IT services auditor and manipulates a company's physical security into letting him into the building.
- **Quid-Pro-Quo:** This is a strategy like Baiting but instead of trading goods, attackers tend to exchange services for their victim to share classified information.
- **Tailgating:** This is a strategy that attackers tend to use in mid-sized businesses, where they engage in conversations with employees and use this show of familiarity to get passed security. In large companies, this usually doesn't work as security keys are required at multiple entrances.

Account Alert - TD Canada Trust anguyen93@live.com

From: web@tdcanadatrust.com

 You may not know this sender. | [Mark as safe](#) | [Mark as junk](#)

Sent: March 16, 2010 12:27:03 PM

To: [REDACTED]



Dear [REDACTED],

This e-mail has been sent to you by **TD Canada Trust** inform you that we were unable to verify your account details. This might be due to either of the following reasons:

1. Submitting incorrect information during register process.
2. A recent change in your personal information. (eg: address, phone)

Due to this, to ensure that your **EasyWEB** service is not interrupted, we request you to confirm and update your information today by following the link below

<https://easyweb.tdcanadatrust.com/verifyloginaccess?id=3529-DwTmqKKz28puser=anguyen93@live.com> 

If you have already confirmed your information then please disregard this message.

Regards,
TD Canada Trust member services

Thanks for your cooperation.

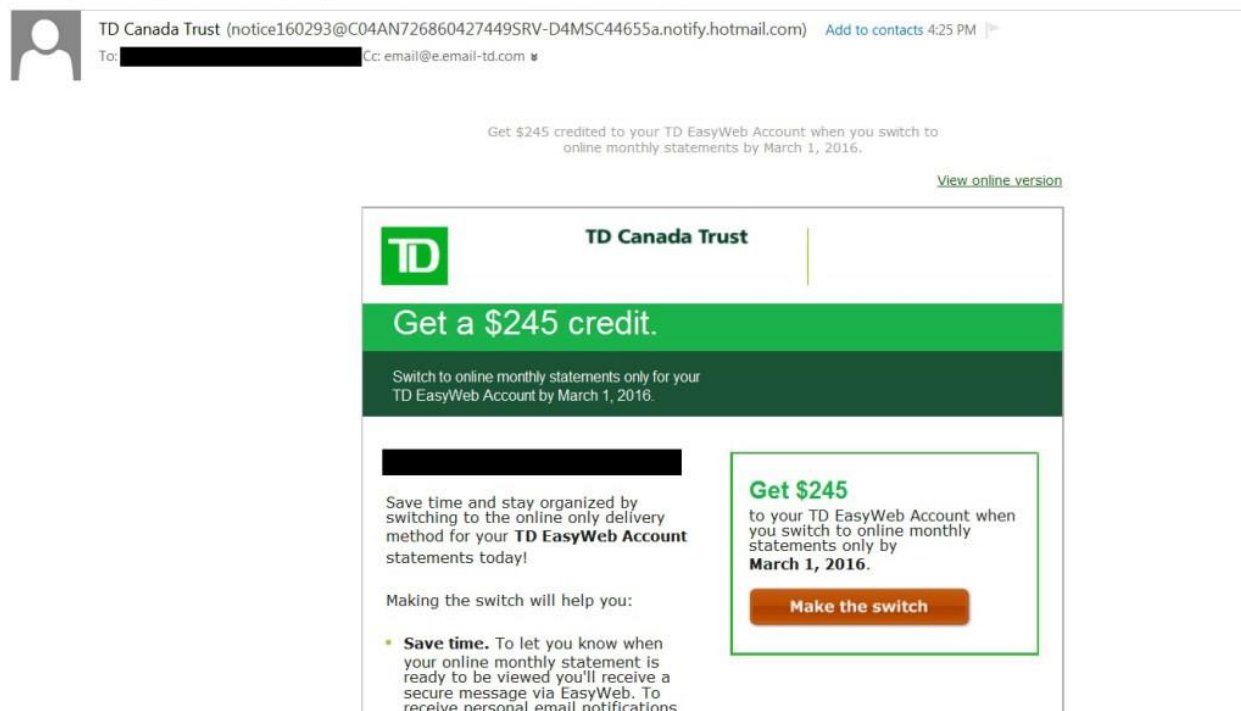
TD Group Financial Services site - Copyright © TD

Most used practice of social engineers is performing the phishing scam. This scam is widely used and is the most clever and efficient way to confuse the people new to technology. A lot of these scams happen through email as emails can be dressed up very easily

as compared to humans. An example would explain this much better.

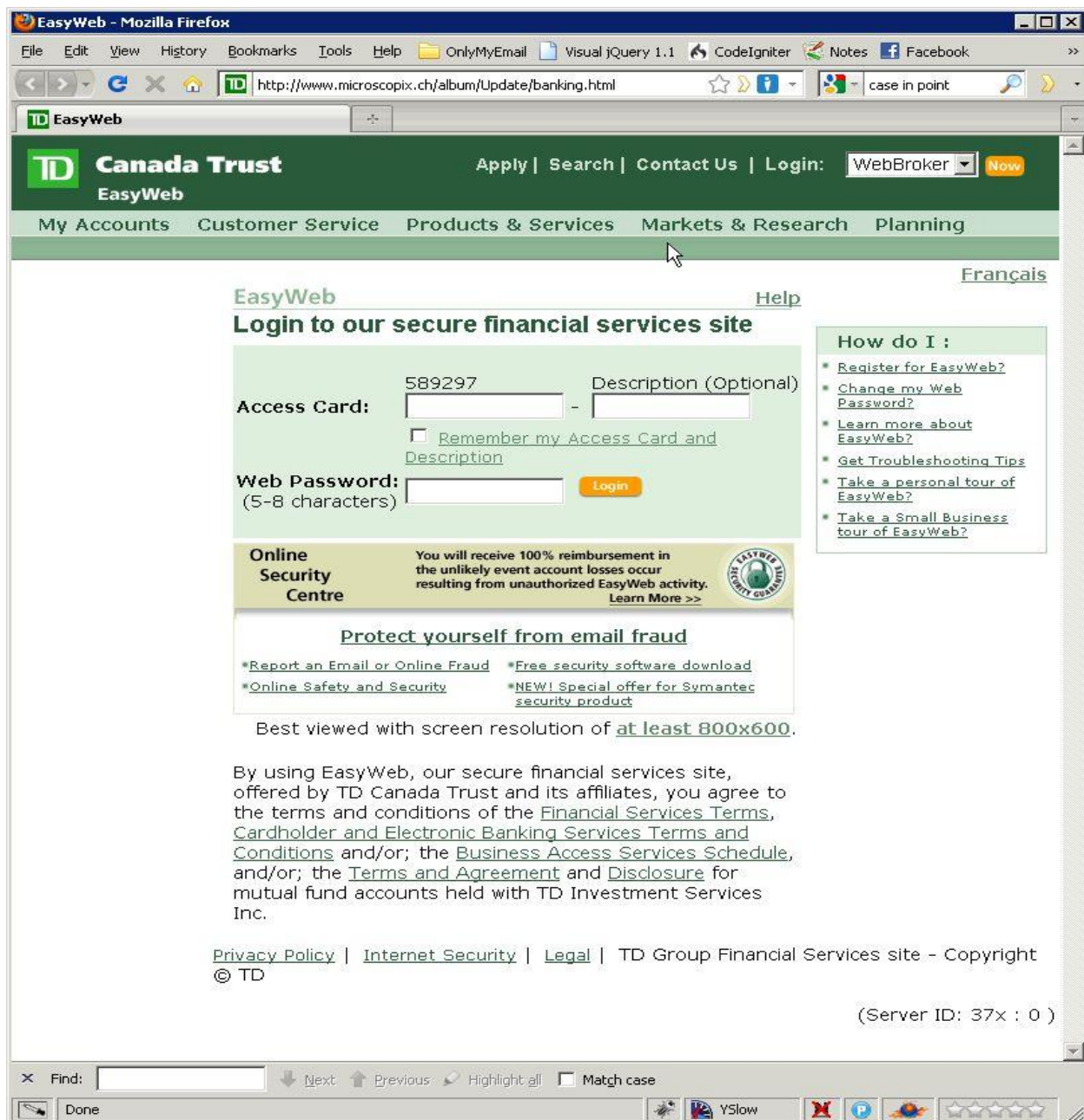
Paying attention to small details on the above image of an email, one can tell that this email is authentically from TD Canada Trust as the email it is sent from has an official server name. There is adequate indentation for paragraphs and bullet points. Words that need to be highlighted are bolder. There are no spelling mistakes. The link that directs the user is 'https' showing that it is a secure verified URL. These attributes mentioned distinguish authentic emails from scams. Now let's look at a scam email from a social engineer.

[Notify: * Save time and stay organized *] New Statements Ready !



In this email shown above, one can easily identify this as an authentic and real email from TD Canada Trust looking at its superbly real looking layout. BUT this email is a scam. The engineer who made this email was careful to add buttons so that the insecure http links can be hidden. Once the user clicks these buttons, the user will be directed to the unofficial TD website that looks like the real website. We'll talk about the website later but if you pay attention to the sender of this email and the subject line, it becomes clear to us that this is a fraudulent email. The sender's email does not have a verified server name. The server name has a bunch of characters to make it random. The subject line also has unnecessary special characters to distinguish from other emails and stand out as a scam. Looking at some websites now will help us understand these scams even better.

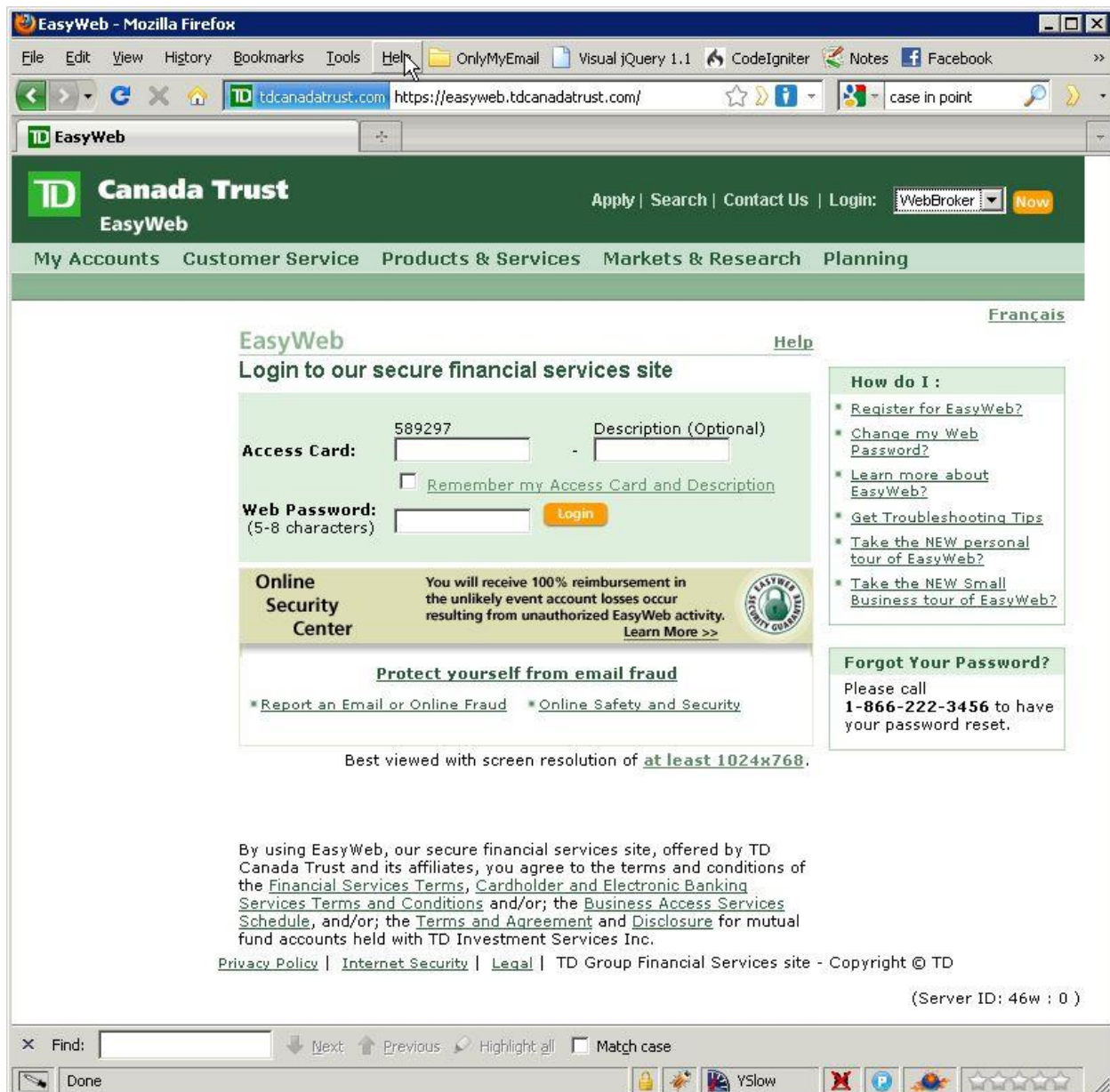
Websites are the tool where these engineers perform the real deal. The scam emails are the pathway to their main plot. Once these emails direct users to websites, those websites tend to ask credentials to log in, those credentials are crucial for hackers as then they can use them on real websites and go in to classified information. An example will explain it more thoroughly.



Above here is an example of a fake website which is infact very similar (we'll look at the real website after) to the athentic TD Canada website. This website might have all the real functionalities but its login

Information panel is the real trap. Once any user enters their login information, the hacker can use those credentials to login to the real website (shown below) and hack into their bank data.

Looking at the URL, we see it is not a secure website because of the 'http' and also, we can read that the website name is 'microscopix' instead of TD's easyweb URL. These two simple pieces of information give away that this is an attack from a social engineer.



The webpage above is the real TD Canada website. We can see how both the websites layout is more

than 90% the same, from the WebBroker login to privacy policy infringement. This makes users like us be very careful in whatever we deal with on the World Wide Web when it comes to secretive information like banking.

Social Engineering has been a considerably effective way of hacking and often times is successful, if not very successful. Billions to trillions of money has been stolen in the past year of 2016 but only looking at social engineering side of hacking, let's look at how much attackers benefitted. According to SC Media from UK,

“The results revealed that 60 percent of surveyed security leaders say their organizations were or may have been victim of at least one targeted social engineering attack in the past year, and 65 percent of those who were attacked say that employees' credentials were compromised as a result of the attacks.”(www.scmagazineuk.com)

Wow, 65% of those attacks were compromised, that's too big of a number and it shows how effective and easy it is for these attackers.

According to a survey from techbeacon, 66% of professionals surveyed identified social engineering as the top threat in the cyber security world. About 200 business and technology professionals classified that their organizations are biggest victims of social engineering. Organizations worldwide are forced to spend more for security breaches because of this hacking era costing up to \$15 million for US companies on annual basis.

Social Engineering is a wide term for an extensive variety of systems utilized by criminal aggressors that endeavor the human component. While digital assaults consolidate a scope of various strategies, plainly there is one extremely basic hazard denominator: us people, or clients.

According to the Verizon 2015 DBIR report, humans, or users, account for 90% of security incidents:

While the threats against us may “seem” innumerable, infinitely varied, and ever-changing, the reality is they aren't. The common denominator across the top four patterns of security incidents – accounting for nearly 90% of incidents – is people. Whether it's goofing up, getting infected, behaving badly or losing stuff.

Symantec and Cisco recently released reports that echo Verizon's findings. The Symantec 2015 Internet Security Threat Report noted that spearphishing, which targets humans, was on the increase:

Almost no company, whether large or small, is immune to spear-phishing. Five out of six large (2,500 + employees) companies were targeted with spearphishing attacks during 2014 – a 40 percent increase over the previous year. Small and medium-sized businesses also saw an uptick, with attacks increasing 26 percent and 30 percent, respectively.

Cisco's 2015 Annual Report noted:

Adversaries are committed to continually refining or developing new techniques that can evade detection and hide malicious activity. Meanwhile, the defenders –namely, security teams –must constantly improve their approach to protecting the organization and users from these increasingly sophisticated campaigns. Caught in the middle are the users. But now, it appears they not only are the targets, but also complicit enablers of attacks.

References:

<http://blog.willis.com/2016/01/social-engineering-is-bigger-than-hacking-but-countermeasures-work/>

<https://techbeacon.com/38-cybersecurity-stats-matter-most>

<http://www.networkworld.com/article/3105496/security/how-well-does-social-engineering-work-one-test-returned-150.html>

<https://www.forbes.com/sites/laurashin/2017/01/04/be-prepared-the-top-social-engineering-scams-of-2017/#683c80917fec>

<http://www.csoononline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html>

<https://www.scmagazineuk.com/60-of-enterprises-were-victims-of-social-engineering-attacks-in-2016/article/576060/>

Incident Handling

What is incident handling?

Incident handling is a generalized term that refers to the response by a person or organization to an attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster. This paper will provide a logical approach to handling two common forms of attack - virus outbreak and system compromise. The method that this article will propose includes the following sequence of steps that should be followed in the case of all types of attack. (Symantec.com)

ACARM (Alert Correlation, Assessment and Reaction Module) is an alert correlation software which can significantly facilitate analyses of a traffic in computer networks. It is responsible for collection and correlation alerts sent by network and host sensors also referred to as *NIDS* and *HIDS* respectively. Correlation process aims to reduce the total number of messages that need to be viewed by a system administrator to as few as possible by merging similar events into groups representing logical pieces of malicious activity. ACARM-ng is an open source technology implemented to detect an incident. ACARM is an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). (acarm.wcss.wroc.pl)

Advantages of Network based Intrusion Detection Systems:

1. **Lower Cost of Ownership:** Network based IDS can be deployed for each network segment. An IDS monitor's network traffic destined for all the systems in a network segment. This nullifies the requirement of loading software at different hosts in the network segment. This reduces management overhead, as there is no need to maintain sensor software at the host level.
2. **Easier to deploy:** Network based IDS are easier to deploy as it does not affect existing systems or infrastructure. The network-based IDS systems are Operating system independent. A network based IDS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running.
3. **Detect network based attacks:** Network based IDS sensors can detect attacks, which host-based sensors fail to detect. A network based IDS checks for all the packet headers for any malicious attack. Many IP-based denial of service attacks like TCP SYN attack, fragmented packet attack etc. can be identified only by looking at the packet headers as they travel across a network. A network based IDS sensor can quickly detect this type of attack by looking at the contents of the packets at the real time.
4. **Retaining evidence:** Network based IDS use live network traffic and does real time intrusion detection. Therefore, the attacker cannot remove evidence of attack. This data can be used for forensic analysis. On the other hand, a host-based sensor detects attacks by looking at

the system log files. Lot of hackers are capable of making changes in the log files so as to remove any evidence of an attack.

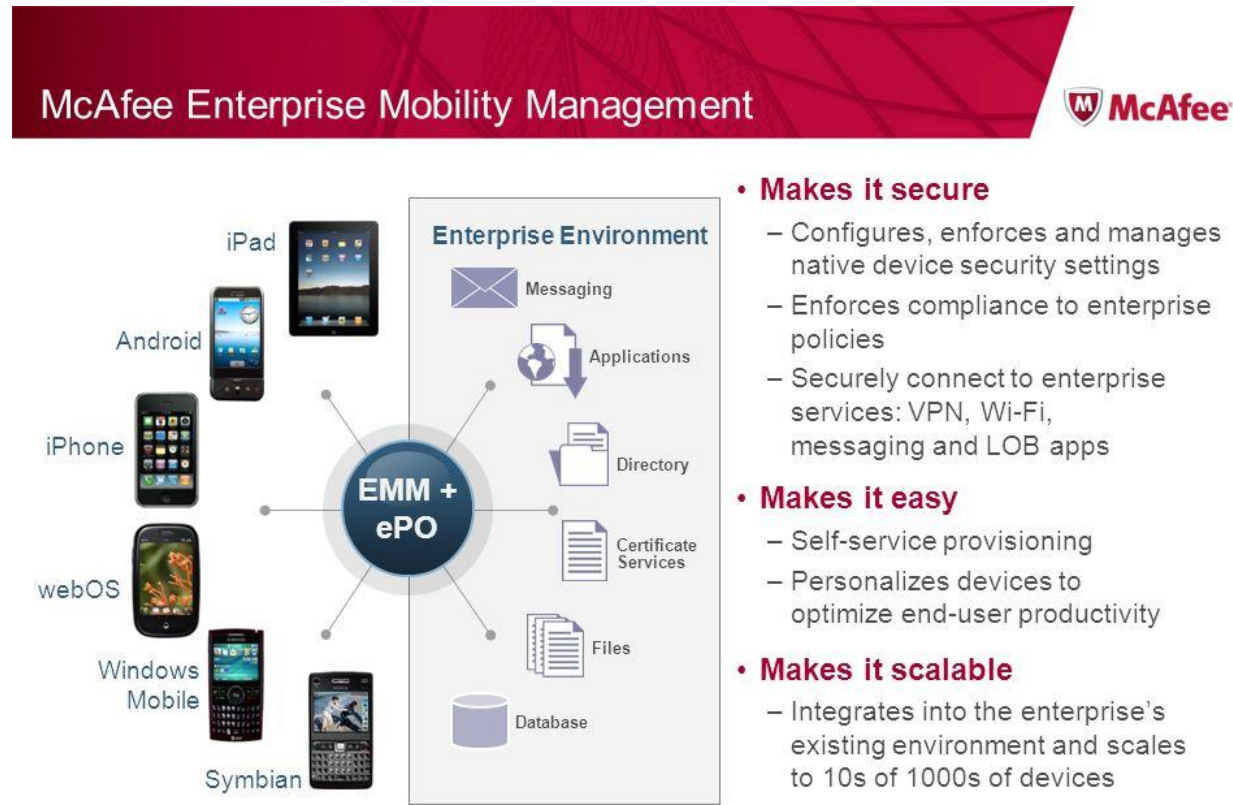
5. Real Time detection and quick response: Network based IDS monitors' traffic on a real time. So, network based IDS can detect malicious activity as they occur. Based on how the sensor is configured, such attack can be stopped even before they can get to a host and compromise the system. On the other hand, host based systems detect attacks by looking at changes made to system files. By this time critical systems may have already been compromised.
6. Detection of failed attacks: A network based IDS sensor deployed outside the firewall (as shown in picture1 above) can detect malicious attacks on resources behind the firewall, even though the firewall may be rejecting these attempts. This information can be very useful for forensic analysis. Host based sensors do not see rejected attacks that could never hit a host inside the firewall.

The main disadvantage of intrusion detection systems is their inability to tell friend from foe. Users inside the system may have harmless activity flagged by the intrusion detection system, resulting in a lock-down the network for an undetermined period of time until a technical professional can be on-site to identify the problem and reset the detection system. To a business dependent on swift action for deadline oriented material, this can cause a drastic loss of revenue and client confidence, as partners may take business elsewhere to a company with a more reliable network.

What is McAfee?

McAfee is a firewall that's purpose is to analyze your defenses and check if your device is vulnerable or not. McAfee performs the same functions as windows some may say, but McAfee makes these alerts more prominent.

McAfee is a firewall that's purpose is to analyze your defenses and check if your device is vulnerable or not. McAfee performs the same functions as windows some may say, but McAfee makes these alerts more prominent.



20

August 30, 2015

McAfee is an international security software company that is one of the world's largest security technology company.

Integration of Endpoint Encryption and ePO

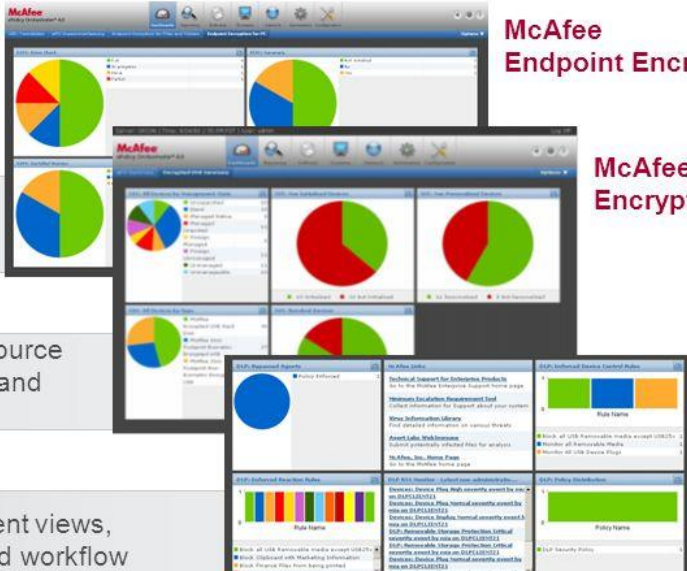


Automation of monitoring, reporting, and auditing **Reduces Costs!**

1 Single console endpoint deployment and management

2 Single consolidated source for incident response and reporting

3 Comprehensive incident views, case management and workflow



McAfee Endpoint Encryption

McAfee Encrypted USB

McAfee DLP

27

Advantages of McAfee:

- This antivirus is easy to use and its latest version is easier and faster than its old versions. Hence, the antivirus doesn't consume large space and helps your PC work faster.
- McAfee antivirus tools are updated with time and its latest versions are really improved. Its firewall feature offers optimal protection when you utilize the internet.
- If you are unaware of technical processes, McAfee is the perfect guide for you. Using the color coding, it provides the users with simple messages.
- The efficient virus protection of McAfee blocks virus within a few seconds only. It can detect every virus, malware by offering a real-time protection called Artemis which scans all files and detects the virus if there is any. Alongside files, it scans the specific URL, IP addresses and the domain data too before saving a file.
- Unlike its previous versions, the latest McAfee antivirus version doesn't slow down the PC while it is booting. This version really performs better.
- Free trial packs are another benefit of choosing McAfee antivirus. Once you get satisfied after using the trial version, you can simply buy the paid version.

- In terms of pricing, McAfee is really a lesser expensive one than other products available in the market.
(www.medium.com/@billyjohns247)

Dis-Advantages of McAfee:

- In accordance with the analysis and comparisons done by TopTenReviews.com, McAfee antivirus is not considered as the fastest antivirus among all antivirus software, as it consumes lots of memory, whether in terms of real-time protection or during the scan.
- According to the aforementioned site, in comparison with other antivirus programs, McAfee is not the most efficient solution for the users.
- Using a huge amount of memory during scanning is another negative point of this antivirus. The duration of full scan perhaps takes a long time. Well, if little memory is consumed by this program during scanning, you could certainly do many tasks simultaneously alongside finishing the scan. Nevertheless, the use of memory is really high and so you basically require leaving your PC alone for finishing the scan procedure.
(www.medium.com/@billyjohns247)

**mcafee.com/us/business-home.aspx*

Include the cost of implementation, including the cost of purchase of the equipment



[Business Home](#) > [Services](#) > [Foundstone Services](#) >

Incident Response & Forensics

Detect and deflect incidents with our Detection and Response team

[Call: 1-877-913-6863](#) [Contact Us](#) [Emergency Services](#)



Overview

Security incidents and losses are on the rise, yet many organizations don't have a plan in place to diagnose and handle a breach. While you can't prevent every possible incident, our Detection and Response team can help you to respond quickly and minimize damage and downtime when attacks and exploits occur. We take a comprehensive and proactive approach to help you protect, detect, correct, and adapt.



Experiencing a Breach?

Contact Foundstone emergency response
now
Phone: 1-877-913-6863

								
Overall Ranking	1st	2nd	3rd	T-4th	T-4th	T-6th	T-6th	T-6th
Lowest Price	\$39.95	\$39.95	\$39.99	\$49.99	\$39.95	\$39.99	\$39.99	Sale: \$34.99
AV-Test Certified	✓	✓	✓	✓	✓	✓	✓	✓
Virus Bulletin 100 Windows 7	✓	✓	✓		✓	✓	✓	
Virus Bulletin 100 Windows XP	✓	✓	✓	✓	✓	✓	✓	✓
ICSA Labs Certification Windows 7	✓	✓	✓		✓	✓		✓
Anti-Virus, Anti-Malware, Anti-Phishing, Anti-Rootkit,	✓	✓	✓	✓	✓	✓	✓	✓

References:

<https://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-61-draft-computer-security-incident-handling-guide-2012.pdf>

<https://countuponsecurity.com/2012/12/21/computer-security-incident-handling-6-steps/>

<https://www.sans.org/score/incident-forms>

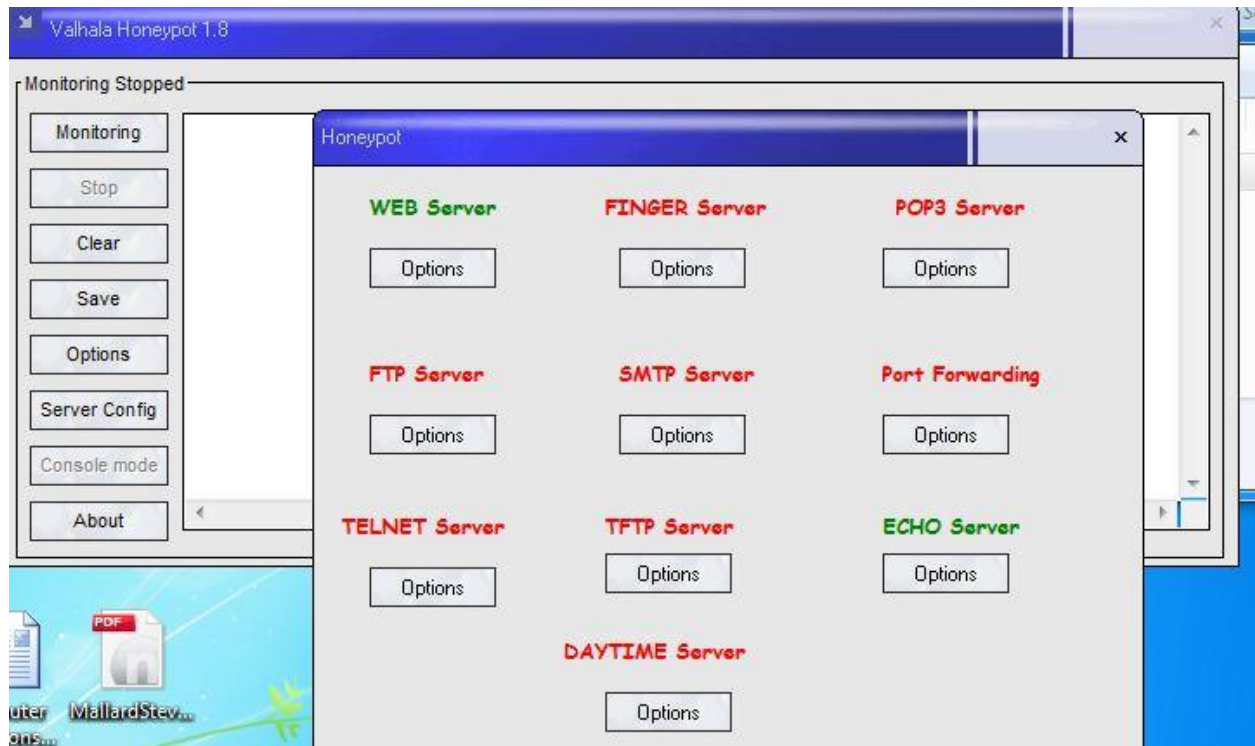
<https://www.rapid7.com/solutions/incident-detection-and-response/>

http://www.uvm.edu/~transctr/pdf/netc/netcr37_00-7.pdf

<https://www.mcafee.com/us/business-home.aspx>

Honeypot Software

Honeypot is a computer security application that is set to detect and deflect attempts at unauthorized use of information systems.



A honeypot is a computer system that is set up to act as a decoy to lure cyberattackers. Generally, it consists of a computer, applications, and data that simulate the behavior of a real system that appears to be part of a network but is actually isolated and closely monitored. All communications with a honeypot are considered hostile, as there's no reason for legitimate users to access a honeypot. Viewing and logging this activity can provide an insight into the level and types of threat a network infrastructure faces while distracting attackers away from assets of real value.

Based on their design and deployment, honeypots are classified as either production or research honeypots. Research honeypots are run to enable close analysis of hacker activity and how attacks develop and progress in order to learn how to better protect systems against them. Data placed in a honeypot with unique identifying properties can also help analysts track stolen data and identify connections between different participants in an attack.

Production honeypots are placed inside a production network with other production servers in the role of a decoy as part of a network intrusion detection system (IDS). They are designed to appear real and contain information or a resource of value with which to attract and occupy hackers. This ties up the attacker's time and resources, hopefully giving administrators time to assess and mitigate any vulnerabilities in their actual production systems. The information gathered from the honeypot can also be useful in catching and prosecuting those behind an attack. Researchers suspect that some cybercriminals also use honeypots to gather intelligence about researchers, act as decoys and to spread misinformation.

High-interaction honeypots imitate the activities of a production system and capture extensive information -- pure honeypots are full-fledged production systems using a tap on the honeypot's link to the network. The goal of high-interaction honeypots is for the attacker to gain root access on the machine, and then study what he or she does. An attacker with root access has access to all commands and files on a system, so this type of honeypot carries the greatest risk but also has the greatest potential for collecting information. Low-interaction honeypots simulate only the services frequently targeted by attackers and so are less risky and less complex to maintain. Virtual machines are often used to host honeypots so the honeypot can be restored more quickly if it is compromised. Two or more honeypots on a network form a honeynet, while a honeyfarm is a centralized collection of honeypots and analysis tools.

(techtarget.com)

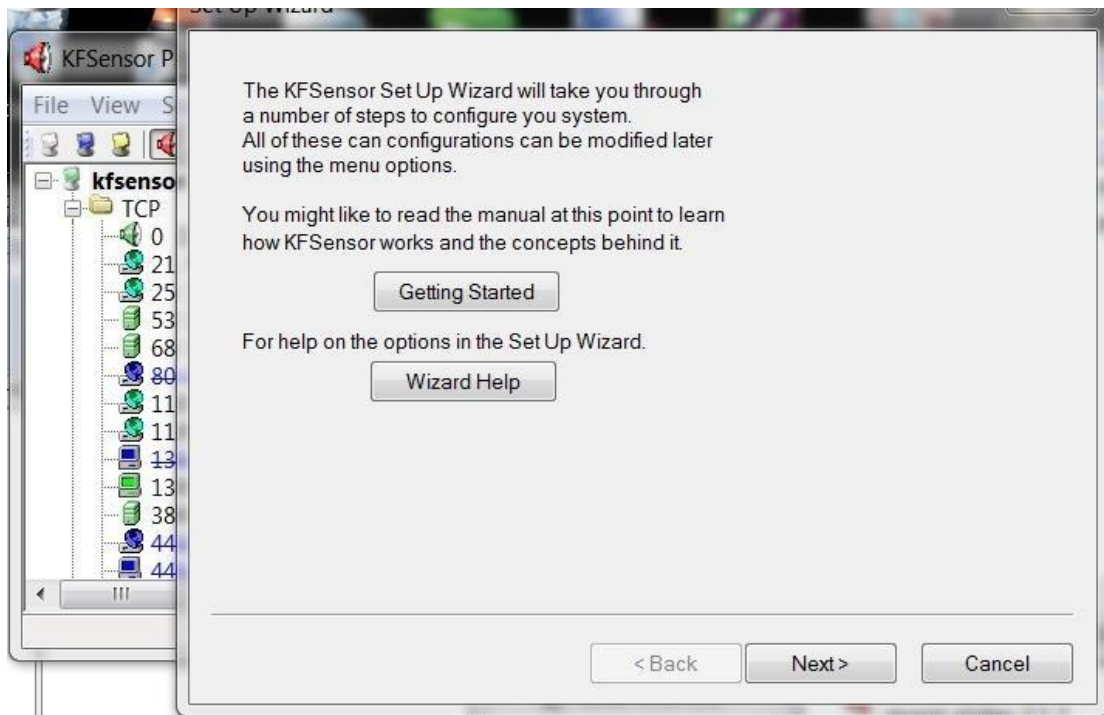
Requirements for Honeypot Software

Step 1: Install KFSensor

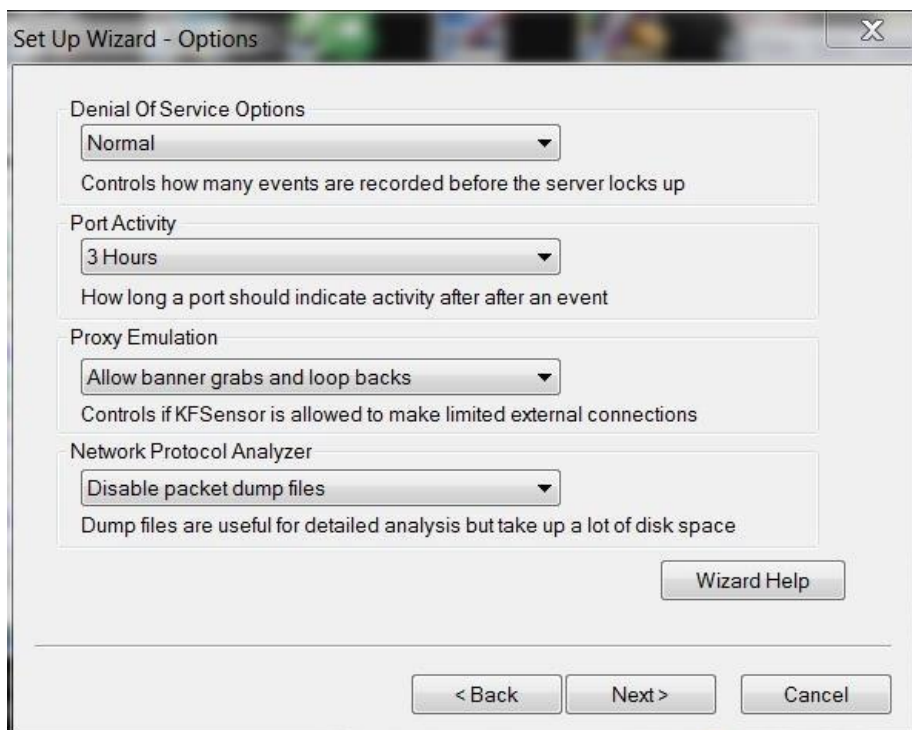
KFSensor enables the user to have an authentic windows system hosting honeypot software, also usable on Kali Linux installed earlier for assignment#1.

Once installed, KFSensor should be ran as administrator privileges, and followed through with the set up wizard.

Choose all native services to experience Honeypot software at its maximum potential.

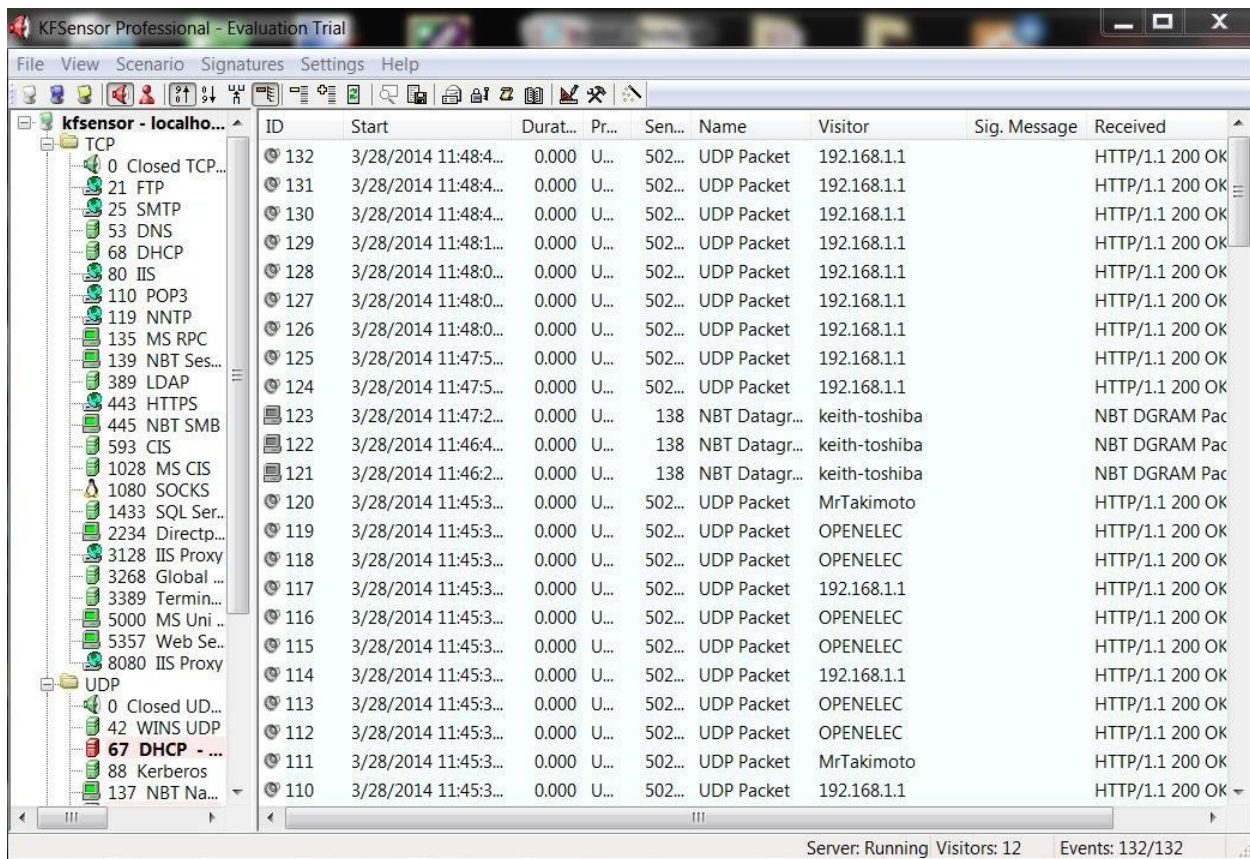


Step 2: Choose Options



For choosing custom options, it is suggested to stay put with the defaults. The last option, Network Protocol Analyzer, gives us the opportunity to capture packets like what we did in online activity 2 with WireShark software. It does warn you that it will take plenty of disk space, thus it is kept disabled for now.

Step 3: Set Up Your Honeypot and Watch

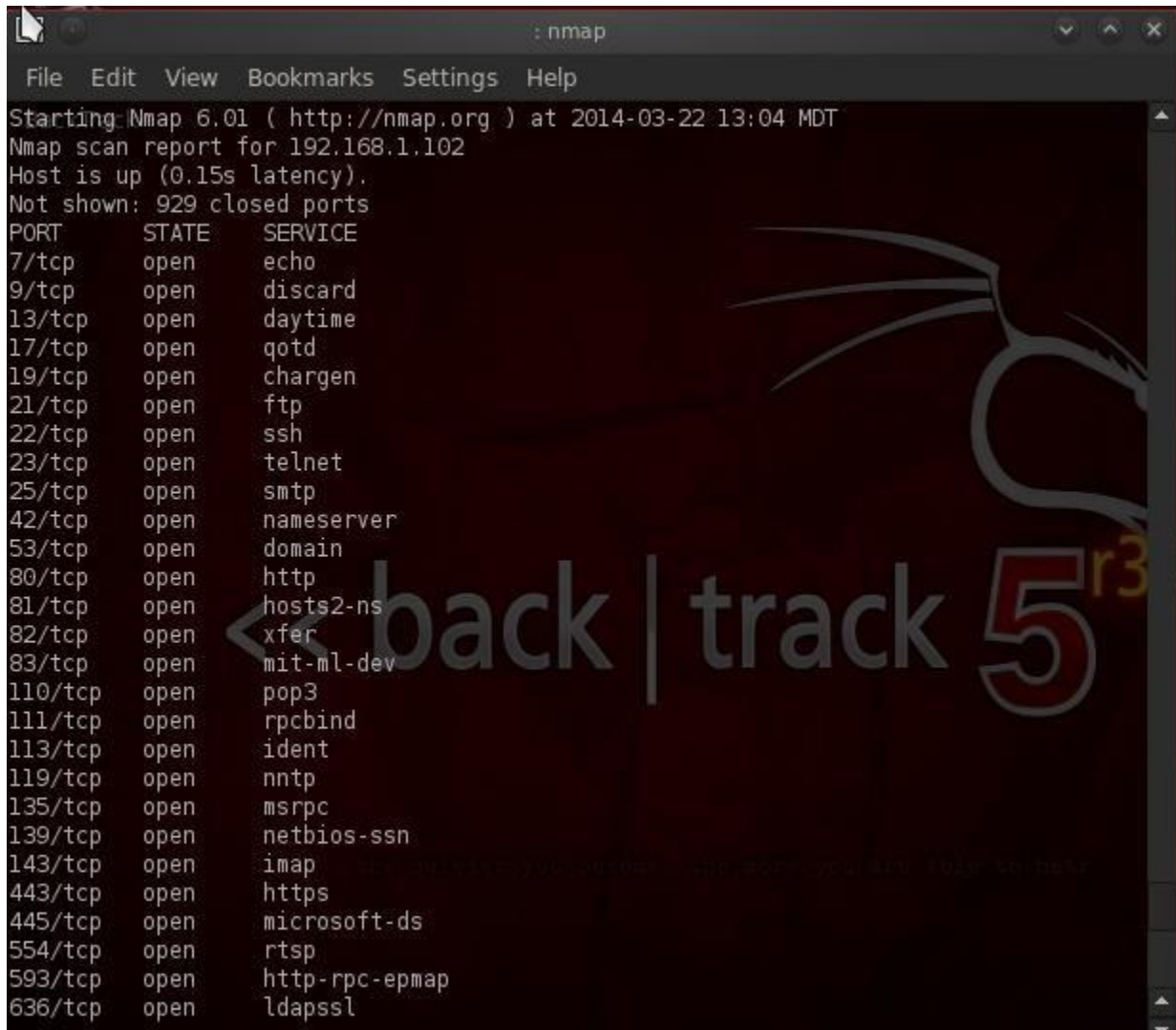


The screenshot shows the KFSensor Professional - Evaluation Trial interface. On the left, there is a tree view of network protocols. The main pane displays a list of network events with columns: ID, Start, Duration, Priority, Sent, Name, Visitor, Signature, Message, and Received. The status bar at the bottom indicates 'Server: Running Visitors: 12 Events: 132/132'.

ID	Start	Durat...	Pr...	Sen...	Name	Visitor	Sig. Message	Received
132	3/28/2014 11:48:4...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
131	3/28/2014 11:48:4...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
130	3/28/2014 11:48:4...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
129	3/28/2014 11:48:1...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
128	3/28/2014 11:48:0...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
127	3/28/2014 11:48:0...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
126	3/28/2014 11:48:0...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
125	3/28/2014 11:47:5...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
124	3/28/2014 11:47:5...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
123	3/28/2014 11:47:2...	0.000	U...	138	NBT Datagr...	keith-toshiba		NBT DGRAM Pac
122	3/28/2014 11:46:4...	0.000	U...	138	NBT Datagr...	keith-toshiba		NBT DGRAM Pac
121	3/28/2014 11:46:2...	0.000	U...	138	NBT Datagr...	keith-toshiba		NBT DGRAM Pac
120	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	MrTakimoto		HTTP/1.1 200 OK
119	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC		HTTP/1.1 200 OK
118	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC		HTTP/1.1 200 OK
117	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
116	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC		HTTP/1.1 200 OK
115	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC		HTTP/1.1 200 OK
114	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK
113	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC		HTTP/1.1 200 OK
112	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	OPENELEC		HTTP/1.1 200 OK
111	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	MrTakimoto		HTTP/1.1 200 OK
110	3/28/2014 11:45:3...	0.000	U...	502...	UDP Packet	192.168.1.1		HTTP/1.1 200 OK

Once the wizard is completed, an application launches that should appear like this.

Step 4: Sacn with Nmap



```
: nmap
File Edit View Bookmarks Settings Help
Starting Nmap 6.01 ( http://nmap.org ) at 2014-03-22 13:04 MDT
Nmap scan report for 192.168.1.102
Host is up (0.15s latency).
Not shown: 929 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  ident
119/tcp   open  nntp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
```

As we look at the target, lets do SYN scan:

Nmap -sS 192.168.1.102

Through this we find numerous ports open.

Going back to Honeypot, we see an alert for a port scan. Most IDS consider many packets coming in in rapid succession from one IP to a possible port scan. It is thus recommended to slow your scan down with nmap's built in speed controls.

ID	Start	Durat...	Pr...	Sensor Port	Name	Visitor	Sig. Message	Received
1314	3/28/2014 4:04:47...	0.000	U...	50274	UDP Packet	OPENELEC		HTTP/1.1 200 OK[0D C
1313	3/28/2014 4:04:47...	0.000	U...	50274	UDP Packet	OPENELEC		HTTP/1.1 200 OK[0D C
1312	3/28/2014 4:04:46...	0.000	U...	60877	UDP Packet	192.168.1.112	<?xml version="1.0" ?>	
1311	3/28/2014 4:04:46...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1310	3/28/2014 4:04:46...	0.000	U...	60877	UDP Packet	192.168.1.112	<?xml version="1.0" ?>	
1309	3/28/2014 4:04:47...	0.000	U...	60877	Port Scan ...	192.168.1.112	Possible Port Scan.[0D	
1308	3/28/2014 4:04:46...	0.000	U...	50274	UDP Packet	MrTakimoto		HTTP/1.1 200 OK[0D C
1307	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1306	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	OPENELEC		HTTP/1.1 200 OK[0D C
1305	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	OPENELEC		HTTP/1.1 200 OK[0D C
1304	3/28/2014 4:04:45...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1303	3/28/2014 4:04:43...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1302	3/28/2014 4:04:40...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1301	3/28/2014 4:04:37...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1300	3/28/2014 4:00:46...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1299	3/28/2014 4:00:43...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C
1298	3/28/2014 4:00:40...	0.000	U...	50274	UDP Packet	192.168.1.1		HTTP/1.1 200 OK[0D C

Step 5: Scan with Nikto

`./nikto.pl -h 192.168.1.102`

This system is default installed of MS IIS 7 server. (red flag that might be honeypot)

```

nikto : nikto.pl
File Edit View Bookmarks Settings Help
root@bt: /pentest/web/nikto# ./nikto.pl -h 192.168.1.102
- Nikto v2.1.5

-----
+ Target IP:          192.168.1.102
+ Target Hostname:    192.168.1.102
+ Target Port:        80
+ Start Time:         2014-03-22 13:14:04 (GMT-6)

-----
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Server banner has changed from Microsoft-IIS/7.5 to Microsoft-HTTPAPI/2.0 which may
  suggest a WAF, load balancer or proxy is in place
+ /: Appears to be a default IIS 7 install.
+ 6474 items checked: 0 error(s) and 5 item(s) reported on remote host
+ End Time:          2014-03-22 13:14:26 (GMT-6) (22 seconds)

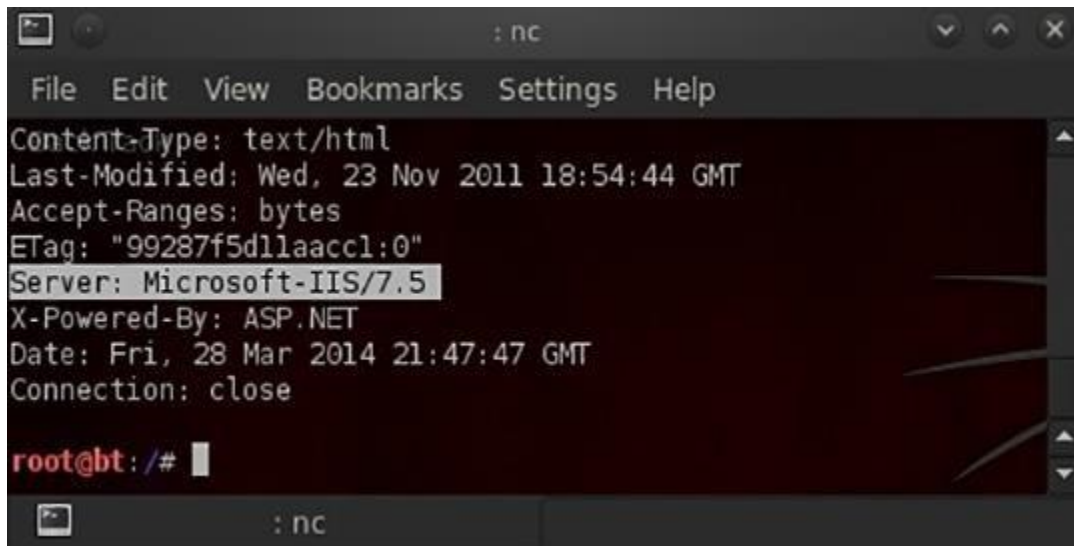
-----
+ 1 host(s) tested
root@bt: /pentest/web/nikto#

```

Step 6: Banner Grab

Lastly, getting banner if there is one.

```
nc 192.168.1.102 80  
HEAD / HTTP/1.0
```

A screenshot of a Netcat terminal window. The window has a title bar with a minimize button, a maximize button, and a close button, followed by the text ': nc'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Bookmarks', 'Settings', and 'Help'. The main area of the window displays the following text: 'Content-Type: text/html', 'Last-Modified: Wed, 23 Nov 2011 18:54:44 GMT', 'Accept-Ranges: bytes', 'ETag: "99287f5d11aaccl:0"', 'Server: Microsoft-IIS/7.5', 'X-Powered-By: ASP.NET', 'Date: Fri, 28 Mar 2014 21:47:47 GMT', and 'Connection: close'. The 'Server: Microsoft-IIS/7.5' line is highlighted with a light blue background. At the bottom of the window, there is a prompt 'root@bt: /# ' followed by a cursor. The status bar at the very bottom shows ': nc'.

References:

<http://www.honeypots.net/honeypots/products>

[https://en.wikipedia.org/wiki/Honeypot_\(computing\)](https://en.wikipedia.org/wiki/Honeypot_(computing))

<http://www.csoononline.com/article/2614083/security/no-honeypot--don-t-bother-calling-yourself-a-security-pro.html>

<https://null-byte.wonderhowto.com/how-to/hack-like-pro-set-up-honeypot-avoid-them-0153391/>