ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

NETWORK FOOTPRINTING (RECONNAISANCE) ΓΙΑ ΤΟΥΣ SERVERS WWW.UNIPI.GR ΚΑΙ DTPS.UNIPI.GR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΞΕΝΑΚΗΣ ΧΡΗΣΤΟΣ
ΦΟΙΤΗΤΗΣ: ΑΘΑΝΑΣΙΟΣ ΣΕΡΒΟΣ
Α.Μ: ΜΤΕ 0926

Περιεχόμενα:

Σκοπός του παραδοτέου

Σκοπός του παραδοτέου είναι η αξιολόγηση της ασφάλειας του τμήματος της πληροφοριακής υποδομής του Πανεπιστημίου Πειραιώς. Η αξιολόγηση αυτή λαμβάνει χώρα σε κανονικές συνθήκες.

Χωρίς να λάβουμε καμία πληροφορία για τη δομή, τη τεχνολογία, τη τοπολογία των πληροφοριακών συστημάτων του πανεπιστημίου, επιχειρήσαμε να εντοπίσουμε κενά στη περίμετρο ασφαλείας του. Με αυτό το τρόπο εντοπίζουμε τις δυνατότητες που έχει ένας εξωτερικός κακόβουλος χρήστης ώστε να πραγματοποιήσει μη εξουσιοδοτημένες ενέργειες.

Σημαντική παράμετρος της διεξαχθείσας εργασίας αποτελεί το γεγονός ότι κανένα μέλος της ομάδας δε διέθετε φυσική πρόσβαση σε οποιοδήποτε πληροφοριακό σύστημα του πανεπιστημίου ή σε κάποιο μεμονωμένο τερματικό αυτού. Επίσης, ουδείς γνώριζε προσωπικά κάποιον διαχειριστή ή οποιοδήποτε άλλο πρόσωπο το οποίο να διαθέτει πρόσβαση στο πληροφοριακό σύστημα ή τον έλεγχο και τη διαχείριση τερματικού συνδεδεμένο σε αυτό.

Η μελέτη ασφάλειας που πραγματοποιήθηκε περιελάμβανε:

- την εύρεση όλων των δικτυακών οντοτήτων που αποτελούν το πληροφοριακό σύστημα και είναι δυνατό να εντοπίσει ένας κακόβουλος τρίτος ο οποίος θέλει να βλάψει την εταιρεία.

- την μελέτη και έρευνα των χαρακτηριστικών των οντοτήτων του πληροφοριακού συστήματος

- τα μέσα σύνδεσής τους και επικοινωνίας τους με το internet αλλά και μεταξύ τους

- μελέτη ασφάλειας τον συγκεκριμένων συστημάτων
  -όσον αφορά τα συστήματα ως αυτοδιαχειριζόμενες οντότητες
  -όσον αφορά τις συνδέσεις των συστημάτων μεταξύ τους αλλά και τους χρήστες

- σενάρια επιθέσεων που υλοποιήθηκαν ή είναι δυνατό να υλοποιηθούν απο τρίτους κακόβουλους

Στην εργασία αυτή θα εστιάσουμε τη μελέτη μας σε δύο servers του πανεπιστημίου. Συγκεκριμένα η μελέτη που κάνουμε αφορά το κεντρικό server με domain unipi.gr και το server που φιλοξενεί το forum του τμήματος ψηφιακών συστημάτων με domain dtps.unipi.gr.

Η μέθοδος καθώς και τα βήματα τα οποία ακολουθήθηκαν στην παρούσα μελέτη ασφάλειας των πληροφοριακών συστημάτων με πρόσβαση μέσω internet από τα domain names www.unipi.gr και dtps.unipi.gr προτείνονται από τον Kevin Orrey, όπως παρουσιάζεται στην ιστοσελίδα http://www.vulnerabilityassessment.co.uk/ και συγκεκριμένα στον ακόλουθο σύνδεσμο http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html.

NETWORK FOOTPRINTING-RECONNAISSANCE

Στο βήμα αυτό ο αναλυτής προσπαθεί να συλλέξει όσο το δυνατόν περισσότερη πληροφορία για το προς μελέτη δίκτυο. Η διαδικασία αυτή έχει δύο μορφές, τη παθητική και την ενεργητική. Μία παθητική επίθεση αποτελεί το καλύτερο εναρκτήριο βήμα καθώς δίνει τη δυνατότητα παράκαμψης των μηχανισμών ελέγχου εισβολής και άλλων μορφών ασφαλείας. Αυτό συνήθως περιλαμβάνει τη διαδικασία ανακάλυψης δημοσίως διαθέσιμης πληροφορίας χρησιμοποιώντας έναν φυλλομετρητή διαδικτύου ή επισκέπτοντας κάποια newsgroups. Από την άλλη μια ενεργητική μορφή επίθεσης περιλαμβάνει ενέργειες οι οποίες μπορεί να καταγράφονται στα log files των συστημάτων όπως για παράδειγμα η απόπειρα αντιγραφής των πληροφοριών DNS.

1. Who is

Η τεχνική του Whois χρησιμοποιείται ευρέως για την αναζήτηση έγκυρων μητρών-registries/βάσεων δεδομένων για να ανακαλύψουμε τον ιδιοκτήτη ενός domain name, μια διεύθυνση IP, ή ένα νούμερο αυτόνομου συστήματος ενός μεγαλύτερου συστήματος που μελετάμε.

- Φορείς Αυθεντικοποίησης
  - IANA - Internet Assigned Numbers Authority
  - ICANN - Internet Corporation for Assigned Names and Numbers.
  - NRO - Number Resource Organisation
  - RIR- Regional Internet Registry – Περιφερειακή Γραμματεία Διαδικτύου
    - AFRINIC - African Network Information Centre
    - APNIC - Asia Pacific Network Information Centre
    - ARIN - American Registry for Internet Numbers
    - LACNIC - Latin America & Caribbean Network Information Centre
    - RIPE - Reseaux IP Européens—Network Coordination Centre – Κέντρο Συντονισμού Δικτύων

- Ιστοσελίδες
  - Central Ops (http://centralops.net/co/)
    - Domain Dossier
    - Email Dossier
  - DNS Stuff (http://www.dnsstuff.com/)

- Online DNS one-stop shop, με την ικανότητα εκτέλεσης πολλών διαφορετικών τύπων ερωτημάτων DNS.

- Fixed Orbit (http://www.fixedorbit.com/)
  - Έλεγχοι αυτόνομων συστημάτων (autonomous system lookups) ενώ υπάρχουν διαθέσιμα και άλλα online εργαλεία.
- Geektools (http://www.geektools.com/)
- IP2Location (http://www.ip2location.com)
  - Επιτρέπει εκτέλεση περιορισμένων IP lookups, εμφανίζοντας πληροφορίες γεωγραφικών τοποθεσιών, λεπτομέρειες του ISP και άλλες σχετικές πληροφορίες.
- Kartoo (http://www.kartoo.com/)
  - Μηχανή αναζήτησης Metasearch η οποία παρουσιάζει γραφικά τα αποτελέσματα.
- MyIPNeighbors.com (http://www.myipneighbors.com)
  - Εξαιρετική ιστοσελίδα που μας δίνει τις λεπτομέρειες της από κοινούς domains σε IP ερωτήματα/ αντίστροφα IP σε DNS resolution (ερώτημα).
- Netcraft (http://news.netcraft.com/)
  - Online εργαλείο αναζήτησης που επιτρέπει ερωτήσεις για πληροφορίες σχετικά με διάφορους hosts.
- Robtex (http://www.robtex.com/)
  - Εξαιρετική ιστοσελίδα που επιτρέπει DNS και AS lookups (αναζητήσεις) που εμφανίζονται με γραφική απεικόνιση των αποτελεσμάτων με δείκτες, A, εγγραφές MX και την συνδεσιμότητα τους με αυτόνομα συστήματα (AS).
- Traceroute.org (http://www.traceroute.org/)
  - Ιστοσελίδα με μια μεγάλη λίστα συνδέσμων για online traceroute πόρους.
- Wayback Machine (http://www.archive.org/index.php)
  - Αποθηκεύει παλαιότερες εκδόσεις ιστοσελίδων, κάνοντας το wayback machine ένα καλό εργαλείο σύγκρισης και μια εξαιρετική πηγή για παλαιότερα αποκατεστημένα δεδομένα από αυτές.
- Whois.net (http://www.whois.net/)

❖ Εργαλεία
- Cheops-ng (http://cheops-ng.sourceforge.net/)
- Country whois (http://www.tamos.com/)
- Domain Research Tool (http://www.domainresearchtool.com/)
- Gnetutil (http://www.culte.org/projets/developpement/gnetutil/)
- Goolag Scanner
- Greenwich (http://www.jodrell.net/files/unsupported/greenwich/)
- Maltego (http://www.paterva.com/web5/)
- GTWhois (http://www.geektools.com/tools.php)
- Sam Spade (http://www.samspade.org/)
- Smart whois (http://www.tamos.com/)
- SpiderFoot (http://www.binarypool.com/spiderfoot/)

Αποτελέσματα:

- Φορείς Αυθεντικοποίησης

  RIPE - Reseaux IP Européens—Network Coordination Centre
  (http://www.db.ripe.net/whois)

  www.unipi.gr (195.251.229.6)
  % This is the RIPE Database query service.
  % The objects are in RPSL format.
  %
  % The RIPE Database is subject to Terms and Conditions.
  % See http://www.ripe.net/db/support/db-terms-conditions.pdf

  % Note: this output has been filtered.
  % To receive output for a database update, use the "-B" flag.

  % Information related to '195.251.224.0 - 195.251.231.255'

  inetnum: 195.251.224.0 - 195.251.231.255
  netname: UOPIRAEUS-NET
  descr: University of Piraeus
  descr: Pireas
  descr: Greece
  country: GR
  admin-c: UoPN1-RIPE
  tech-c: UoPN1-RIPE
  status: ASSIGNED PA
  mnt-by: GRNET-NOC
  mnt-domains: MNT-GRNET-DNS
  mnt-routes: AS12402-MNT
  source: RIPE # Filtered

  role: University of Piraeus NOC
  address: University of Piraeus
  address: 80 Karaoli & Dimitriou St., GR-18534 Piraeus, Greece
  phone: +30 210 414 2174
  fax-no: +30 210 414 2180
  admin-c: JS4607-RIPE
  tech-c: TT1003-RIPE
  remarks: ----------
  remarks: For complains about abuse, spam etc:
  abuse-mailbox: abuse@unipi.gr
  remarks: ----------
  mnt-by: GRNET-NOC
  mnt-by: AS12402-MNT
  nic-hdl: UoPN1-RIPE
  source: RIPE # Filtered

% Information related to '195.251.224.0/21AS12402'

route: 195.251.224.0/21
descr: UOPIRAEUS-NET
descr: University of Piraeus
origin: AS12402
mnt-by: AS12402-MNT
source: RIPE # Filtered

% Information related to '195.251.0.0/16AS5408'

route: 195.251.0.0/16
descr: Aggregated address space announced by AS5408
descr: GRNET
origin: AS5408
mnt-by: GRNET-NOC
source: RIPE # Filtere

http://dtps.unipi.gr/ (195.251.226.211)
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '195.251.224.0 - 195.251.231.255'

inetnum: 195.251.224.0 - 195.251.231.255
netname: UOPIRAEUS-NET
descr: University of Piraeus
descr: Pireas
descr: Greece
country: GR
admin-c: UoPN1-RIPE
tech-c: UoPN1-RIPE
status: ASSIGNED PA
mnt-by: GRNET-NOC
mnt-domains: MNT-GRNET-DNS
mnt-routes: AS12402-MNT
source: RIPE # Filtered

role: University of Piraeus NOC
address: University of Piraeus
address: 80 Karaoli & Dimitriou St., GR-18534 Piraeus, Greece
phone: +30 210 414 2174

fax-no: +30 210 414 2180
admin-c: JS4607-RIPE
tech-c: TT1003-RIPE
remarks: ----------
remarks: For complains about abuse, spam etc:
abuse-mailbox: abuse@unipi.gr
remarks: ----------
mnt-by: GRNET-NOC
mnt-by: AS12402-MNT
nic-hdl: UoPN1-RIPE
source: RIPE # Filtered

% Information related to '195.251.224.0/21AS12402'

route: 195.251.224.0/21
descr: UOPIRAEUS-NET
descr: University of Piraeus
origin: AS12402
mnt-by: AS12402-MNT
source: RIPE # Filtered

% Information related to '195.251.0.0/16AS5408'

route: 195.251.0.0/16
descr: Aggregated address space announced by AS5408
descr: GRNET
origin: AS5408
mnt-by: GRNET-NOC
source: RIPE # Filtered

- Ιστοσελίδες
  - Central Ops (http://centralops.net/co/)
    Domain Dossier: Investigate domains and IP addresses
    - www.unipi.gr

Address lookup

canonical name spider.unipi.gr.
aliases
addresses 195.251.229.6

Domain Whois record

Queried whois.grnet.gr with "-B unipi.gr"...

Query error: **TimedOut**

DNS records

name	class	type	data	time to live
www.unipi.gr	IN	CNAME	spider.unipi.gr	500s (00:08:20)
spider.unipi.gr	IN	MX	preference: 5 exchange: webmail.unipi.gr	500s (00:08:20)
spider.unipi.gr	IN	A	195.251.229.6	500s (00:08:20)
unipi.gr	IN	SOA	server: ns.unipi.gr email: root.unipi.gr serial: 2011033101 refresh: 1200 retry: 7200 expire: 2419200 minimum ttl: 86400	500s (00:08:20)
unipi.gr	IN	MX	preference: 5 exchange: mailhost.unipi.gr	500s (00:08:20)
unipi.gr	IN	NS	ns.unipi.gr	500s (00:08:20)
unipi.gr	IN	NS	sns1.grnet.gr	500s (00:08:20)
unipi.gr	IN	NS	sns0.grnet.gr	500s (00:08:20)
6.229.251.195.in-addr.arpa	IN	PTR	spider.unipi.gr	86400s (1.00:00:00)

-- end --

- http://dtps.unipi.gr/

Address lookup

canonical name dtps.ted.unipi.gr.

aliases

addresses 195.251.226.211

Domain Whois record

Queried whois.grnet.gr with "-B unipi.gr"...

Query error: **TimedOut**

DNS records

name	class	type	data	time to live

dtps.unipi.gr	IN	CNAME	dtps.ted.unipi.gr	500s	(00:08:20)
dtps.ted.unipi.gr	IN	MX	preference: 5 exchange: dtps.ted.unipi.gr	500s	(00:08:20)
dtps.ted.unipi.gr	IN	A	195.251.226.211	500s	(00:08:20)
unipi.gr	IN	SOA	server: ns.unipi.gr email: root.unipi.gr serial: 2011033101 refresh: 1200 retry: 7200 expire: 2419200 minimum ttl: 86400	500s	(00:08:20)
unipi.gr	IN	NS	sns0.grnet.gr	500s	(00:08:20)
unipi.gr	IN	NS	sns1.grnet.gr	500s	(00:08:20)
unipi.gr	IN	NS	ns.unipi.gr	500s	(00:08:20)
unipi.gr	IN	MX	preference: 5 exchange: mailhost.unipi.gr	500s	(00:08:20)
211.226.251.195.in-addr.arpa	IN	PTR	dtps.ted.unipi.gr	86400s	(1.00:00:00)

-- end –

- Netcraft (http://www.netcraft.com/)

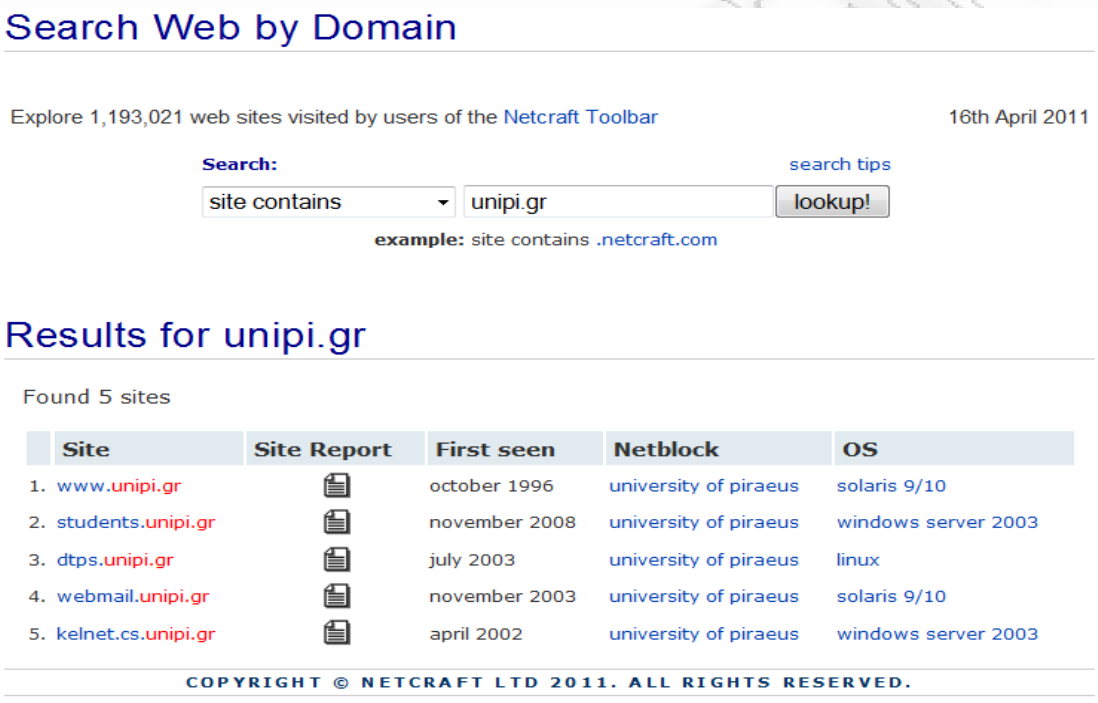
Το Netcraft αποτελεί μια εταιρεία παρακολούθησης του διαδικτύου η οποία καταγράφει το χρόνο λειτουργίας και παρέχει αναγνώριση λετουργικού συστήματος των servers που λειτουργούν στο διαδίκτυο. Η συγκεκριμένη εταιρεία διαθέτει ένα online εργαλείο αναζήτησης το οποίο επιτρέπει σε χρήστες να πραγματοποιούν ερωτήματα στη βάση δεδομένων του για διάφορα συστήματα.

Το online εργαλείο αναζήτησης επιτρέπει wildcard αναζητήσεις που σημαίνει ότι ένας χρήστης μπορεί να εισάγει *unipi* και το αποτέλεσμα που θα επιστραφεί θα περιέχει όλα τα domains τα οποία θα περιέχουν τη λέξη unipi σε αυτό. Το αποτέλεσμα μπορεί να είναι www.unipi.gr αλλά και dtps.unipi.gr επεκτείνοντας τη λίστα των ήδη γνωστών domains. Πηγαίνοντας ένα βήμα παραπέρα ένας χρήστης μπορεί να επιλέξει το συγκεκριμένο σύνδεσμο που έχει επιστραφεί από την αναζήτηση κάτι το οποίο θα αποκαλύψει πολύτιμη πληροφορία όπως:

- IP διεύθυνση
- Ονομασία των servers
- Dns ονόματα από IP διευθύνσεις
- Ιδιοκτήτης του συγκεκριμένου block δικτύου

- Διαχειριστής του domain
- Εγγραφή του domain στο μητρώο

Πρέπει να τονίσουμε ότι αυτός δεν είναι ο μόνος τρόπος να εξάγουμε τη παραπάνω πληροφορία καθώς είναι πολύ εύκολο να βρει ένας επιτιθέμενος εξειδικευμένο λογισμικό με πολύ περισσότερες δυνατότητες το οποίο κυκλοφορεί ελεύθερα διαθέσιμο στο διαδικτύο και να καταφέρει να συγκεντρώσει πολύ περισσότερη πληροφορία.
Εκτελώντας ένα παράδειγμα για να δείξουμε πρακτικά τα παραπάνω, δίνουμε ως είσοδο στο εργαλείο αυτό το domain unipi.gr. Στο παρακάτω σχήμα φαίνονται τα αποτελέσματα που επιστρέφει το online εργαλείο αναζήτησης:



Αποτελέσματα αναζήτησης για το unipi.gr

Όπως αναφέρθηκε και παραπάνω το συγκκεριμένο εργαλείο μπορεί να αποκαλύψει και άλλες χρήσιμες πληροφορίες. Για παράδειγμα, επιλέγοντας την αναφορά για το url www.unipi.gr λαμβάνουμε τις πληροφορίες που φαίνονται στο παρακάτω σχήμα:

Site report for www.unipi.gr

Site	http://www.unipi.gr	**Last reboot**	unknown Uptime graph
Domain	unipi.gr	**Netblock owner**	University of Piraeus
IP address	195.251.229.6	**Site rank**	307028
Country	GR	**Nameserver**	ns.unipi.gr
Date first seen	October 1996	**DNS admin**	root@unipi.gr
Domain Registrar	ripe.net	**Reverse DNS**	spider.unipi.gr
Organisation		**Nameserver Organisation**	
Check another site:		**Netcraft Site Report Gadget**	Google [More Netcraft Gadgets]

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	5-Feb-2011
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	17-Oct-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	26-Aug-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	27-Jun-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	9-Feb-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	7-Feb-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	28-Jan-2010
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	28-Apr-2009
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	12-Jan-2009
University of Piraeus Pireas Greece	195.251.229.6	Solaris 9/10	Apache/2.0.54 Unix DAV/2	26-Sep-2008

Πληροφορία όπως IP διευθύνσεις, λειτουργικό σύστημα του web server κ.α

- Robtex (http://www.robtex.com/)
  - www.unipi.gr

195.251.229							
More information							
It is not listed in any blacklists.							
IP and Domain Information Sources							
Source	**Date**	**Information**					
	########## ###	This information page's creation date					
	########## ###	Blacklistings					
195.251.0.0/16 Aggregated address space announced by AS5408 GRNET AS5408							
195.251.224.0/21 UOPIRAEUS-NET University of Piraeus AS12402 (not announced)							

Base	Record	Name	IP	Reverse	Route	AS
subnetsrv.noc.unipi.gr	ptr		195.251.229.0		195.251.0.0/16	AS5408
			Greece		Aggregated address space announced by AS5408 GRNET	GR-NET Greek Research & Technology Network, http://www.grnet.gr
richesesrv.noc.unipi.gr	ptr		195.251.229.1			
			Greece			
gamondsrv.noc.unipi.gr	ptr		195.251.229.2			
			Greece			
	-		195.251.229.3	(none)		
			Greece			
			195.251.229.4			
			Greece			
dune.unipi.gr	a		195.251.229.5			
			Greece			
ns.unipi.gr	a		195.251.229.5	dune.unipi.gr		
			Greece			
spider.unipi.gr	a		195.251.229.6			
			Greece			
webmail.unipi.gr	a		195.251.229.6	spider.unipi.gr		
			Greece			
www.unipi.gr	cname	spider.unipi.gr	195.251.229.6			
			Greece			
login.unipi.gr	a		195.251.229.7			
			Greece			
vhost.unipi.gr	a		195.251.229.8			
			Greece			
ermis.unipi.gr	a		195.251.229.9			
			Greece			
mailhost.unipi.gr	a		195.251.229.9	ermis.unipi.gr		

			Greece		
pythia.unipi.gr	a		195.251.229.10		
			Greece		
	-		195.251.229.11	(none)	
			Greece		
			195.251.229.12		
			Greece		
			195.251.229.13		
			Greece		
			195.251.229.14		
			Greece		
			195.251.229.15		
			Greece		
			195.251.229.16		
			Greece		
			195.251.229.17		
			Greece		
			195.251.229.18		
			Greece		
			195.251.229.19		
			Greece		
			195.251.229.20		
			Greece		
			195.251.229.21		
			Greece		
			195.251.229.22		
			Greece		
			195.251.229.23		
			Greece		
			195.251.229.24		
			Greece		
			195.251.229.25		
			Greece		
			195.251.229.26		
			Greece		
			195.251.229.27		
			Greece		
			195.251.229.28		
			Greece		
			195.251.229.29		
			Greece		
			195.251.229.30		
			Greece		
			195.251.229.31		

			Greece		
			195.251.229.32		
			Greece		
			195.251.229.33		
			Greece		
			195.251.229.34		
			Greece		
			195.251.229.35		
			Greece		
			195.251.229.36		
			Greece		
			195.251.229.37		
			Greece		
			195.251.229.38		
			Greece		
			195.251.229.39		
			Greece		
			195.251.229.40		
			Greece		
			195.251.229.41		
			Greece		
			195.251.229.42		
			Greece		
			195.251.229.43		
			Greece		
			195.251.229.44		
			Greece		
			195.251.229.45		
			Greece		
			195.251.229.46		
			Greece		
			195.251.229.47		
			Greece		
			195.251.229.48		
			Greece		
			195.251.229.49		
			Greece		
			195.251.229.50		
			Greece		
			195.251.229.51		
			Greece		
			195.251.229.52		
			Greece		
			195.251.229.53		

			Greece			
			195.251.229.54			
			Greece			
			195.251.229.55			
			Greece			
			195.251.229.56			
			Greece			
			195.251.229.57			
			Greece			
			195.251.229.58			
			Greece			
			195.251.229.59			
			Greece			
			195.251.229.60			
			Greece			
			195.251.229.61			
			Greece			
			195.251.229.62			
			Greece			
			195.251.229.63			
			Greece			
subnetnoc.noc.unipi.gr	ptr		195.251.229.64			
			Greece			
richesenoc.noc.unipi.gr	ptr		195.251.229.65			
			Greece			
gamond.noc.unipi.gr	a		195.251.229.66	gamondnoc.noc.unipi.gr		
			Greece			
gamondnoc.noc.unipi.gr	ptr		195.251.229.66			
			Greece			
	-		195.251.229.67	(none)		
			Greece			
			195.251.229.68			
			Greece			
			195.251.229.69			
			Greece			
noc.noc.unipi.gr	a		195.251.229.70	noce0.noc.unipi.gr		
			Greece			
noce0.noc.unipi.gr	cname	noc.noc.unipi.gr	195.251.229.70	noce0.noc.unipi.gr		

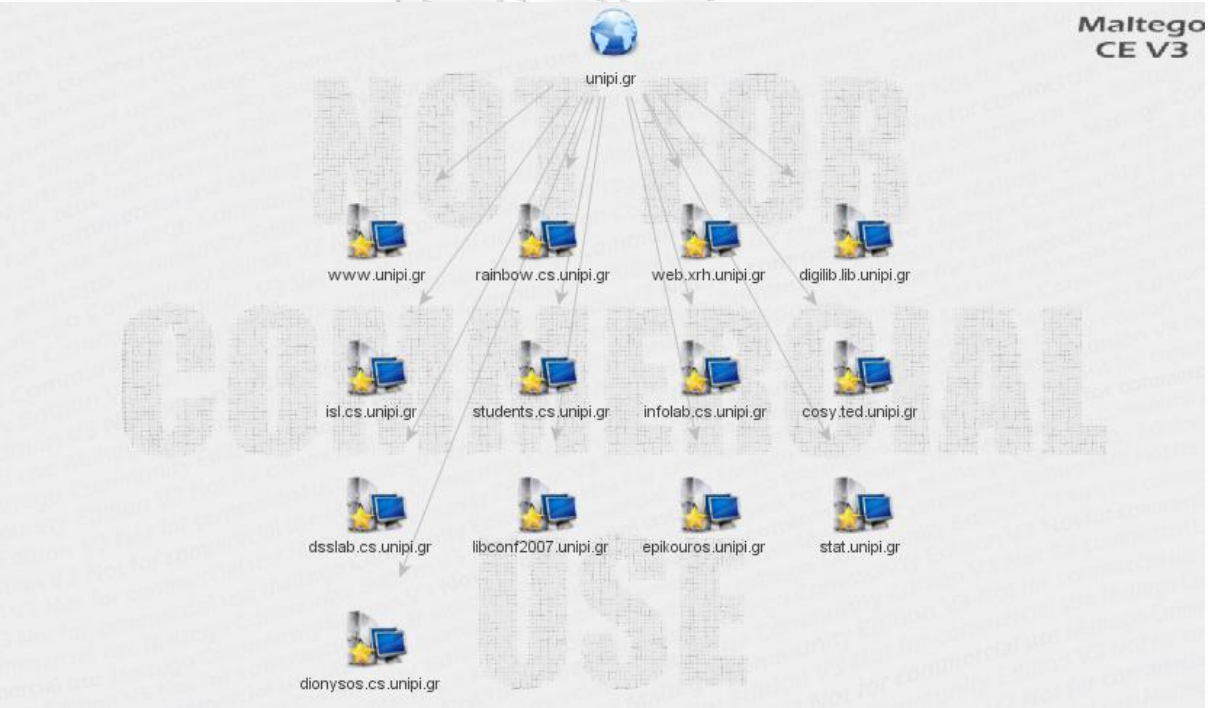
			Greece			
chusuk.noc.unipi.gr	a		195.251.229.71			
			Greece			
giedi.noc.unipi.gr	a		195.251.229.72			
			Greece			
	-		195.251.229.73	(none)		
			Greece			
			195.251.229.74			
			Greece			
			195.251.229.75			
			Greece			
			195.251.229.76			
			Greece			
pythia.noc.unipi.gr	a		195.251.229.77			
			Greece			
	-		195.251.229.78	(none)		
			Greece			
			195.251.229.79			
			Greece			
nocst.noc.unipi.gr	a		195.251.229.80			
			Greece			
tapehost.noc.unipi.gr	a		195.251.229.80	nocst.noc.unipi.gr		
			Greece			
test1.noc.unipi.gr	ptr		195.251.229.81			
			Greece			
test2.noc.unipi.gr	ptr		195.251.229.82			
			Greece			
test3.noc.unipi.gr	ptr		195.251.229.83			
			Greece			
test4.noc.unipi.gr	ptr		195.251.229.84			
			Greece			
	-		195.251.229.85	(none)		
			Greece			
			195.251.229.86			
			Greece			
caladan.noc.unipi.gr	a		195.251.229.87			
			Greece			
ecaz.noc.unipi.gr	a		195.251.229.88			
			Greece			

linoc.noc.unipi.gr	a		195.251.229.89			
			Greece			
	-		195.251.229.90	(none)		
			Greece			
			195.251.229.91			
			Greece			
kyriakos4.noc.unipi.gr	a		195.251.229.92			
			Greece			
zx1.noc.unipi.gr	a		195.251.229.93			
			Greece			
gtdialin.noc.unipi.gr	a		195.251.229.94			
			Greece			
eee-rosa.noc.unipi.gr	a		195.251.229.95			
			Greece			
	-		195.251.229.96	(none)		
			Greece			
newvd.noc.unipi.gr	a		195.251.229.97			
			Greece			
newera.noc.unipi.gr	a		195.251.229.98			
			Greece			
rts.noc.unipi.gr	a		195.251.229.99			
			Greece			
gk.noc.unipi.gr	a		195.251.229.100			
			Greece			
tgt.noc.unipi.gr	a		195.251.229.101			
			Greece			
kyriakos.noc.unipi.gr	a		195.251.229.102			
			Greece			
rosa.noc.unipi.gr	a		195.251.229.103			
			Greece			
sgavala.noc.unipi.gr	a		195.251.229.103	rosa.noc.unipi.gr		
			Greece			
kyriakos2.noc.unipi.gr	a		195.251.229.104			
			Greece			

edulptp.noc.unipi.gr	a	195.251.229.105		
		Greece		
laptop.noc.unipi.gr	a	195.251.229.106		
		Greece		
tgt-z800.noc.unipi.gr	a	195.251.229.107		
		Greece		
agalani.noc.unipi.gr	a	195.251.229.108		
		Greece		
lxe352dn.noc.unipi.gr	a	195.251.229.109		
		Greece		
ds-unipi.noc.unipi.gr	a	195.251.229.110		
		Greece		
sgavala2.noc.unipi.gr	a	195.251.229.110	ds-unipi.noc.unipi.gr	
		Greece		
new-dune.unipi.gr	a	195.251.229.111		
		Greece		
hplj4321.noc.unipi.gr	a	195.251.229.112		
		Greece		
epik.noc.unipi.gr	a	195.251.229.113		
		Greece		
kyriakos3.noc.unipi.gr	a	195.251.229.114		
		Greece		
vassok.noc.unipi.gr	a	195.251.229.115		
		Greece		
fbsdvk.noc.unipi.gr	a	195.251.229.116		
		Greece		
hplj4320.noc.unipi.gr	a	195.251.229.118		
		Greece		
comproom.noc.unipi.gr	a	195.251.229.119		
		Greece		

agallptp.noc.unipi.gr	a	195.251.229.120		
		Greece		
vaio31h.noc.unipi.gr	a	195.251.229.121		
		Greece		
ipphone1.noc.unipi.gr	a	195.251.229.123		
		Greece		
vknwdesk.noc.unipi.gr	a	195.251.229.124		
		Greece		
melampus.noc.unipi.gr	a	195.251.229.125		
		Greece		
okic3530.noc.unipi.gr	a	195.251.229.126		
		Greece		

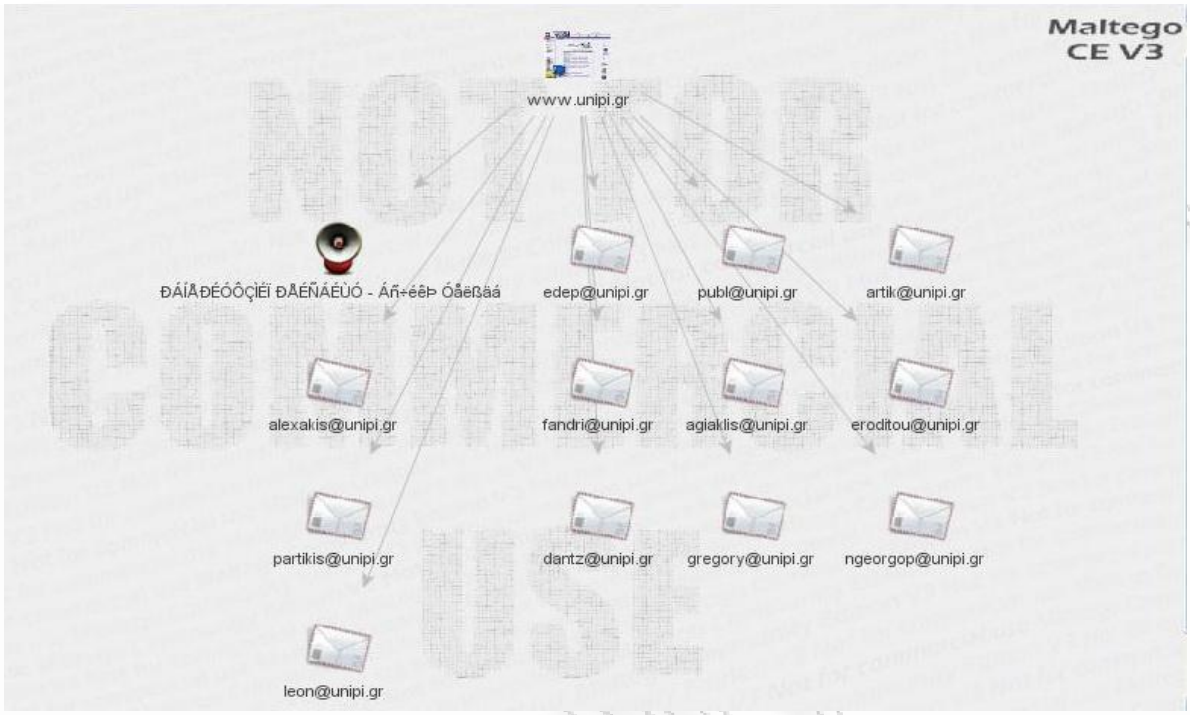
- Εργαλεία
  - Maltego
    - www.unipi.gr
      -



- Other Transforms:

  Mirror: Email addresses found
  To URLs [show Search Engine results]
  To Website [Replace with thumbnail]

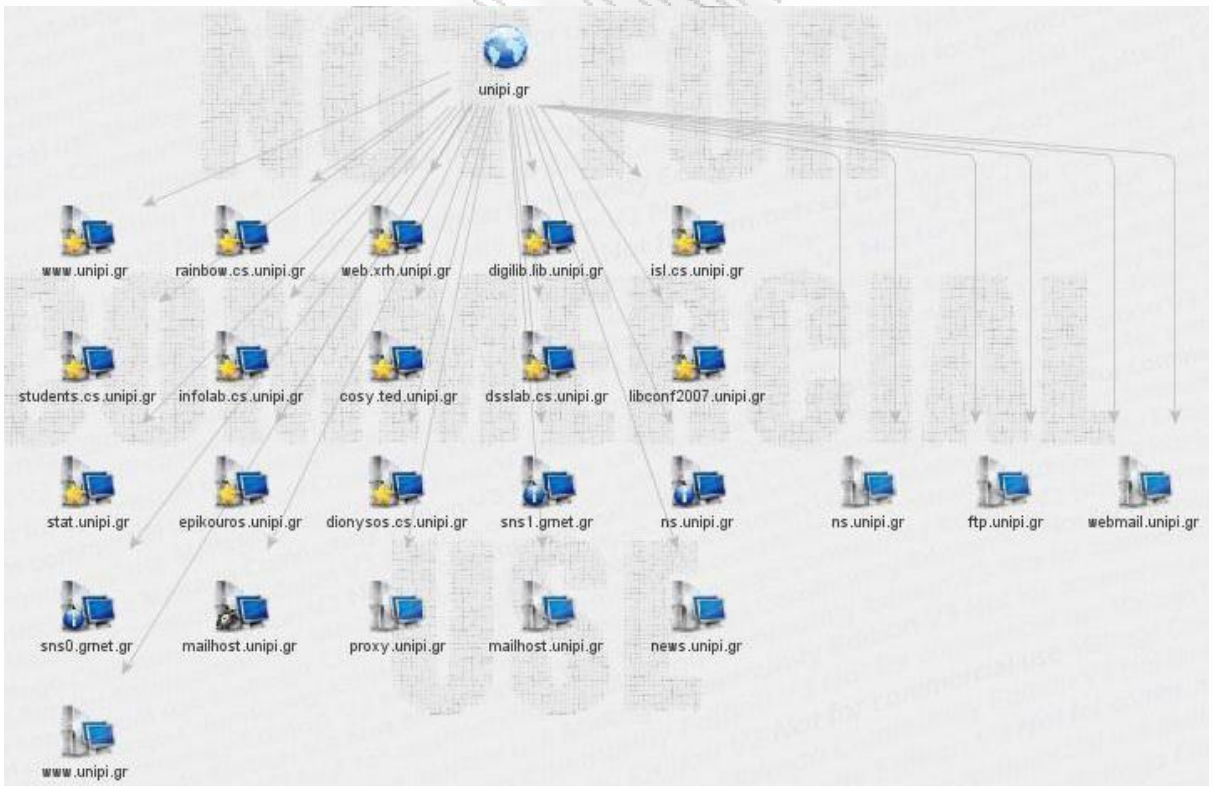
To Website title



- Link in and out of site

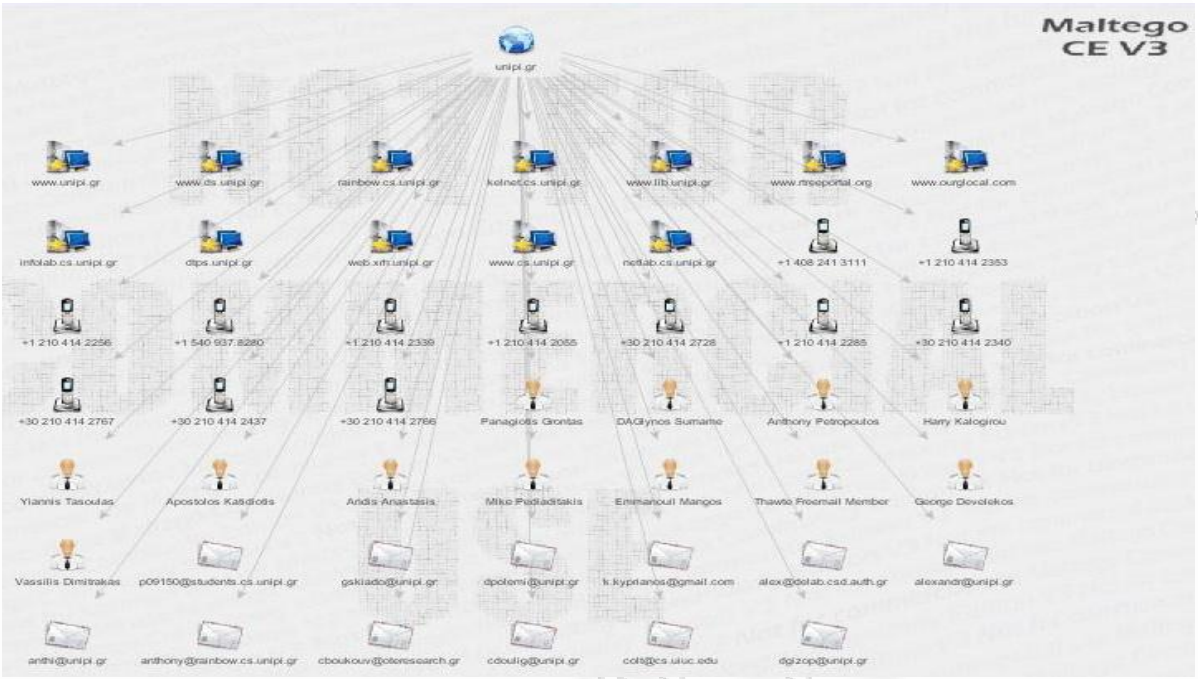
  -Mirror External links found

  -To Website [Incoming links to site]

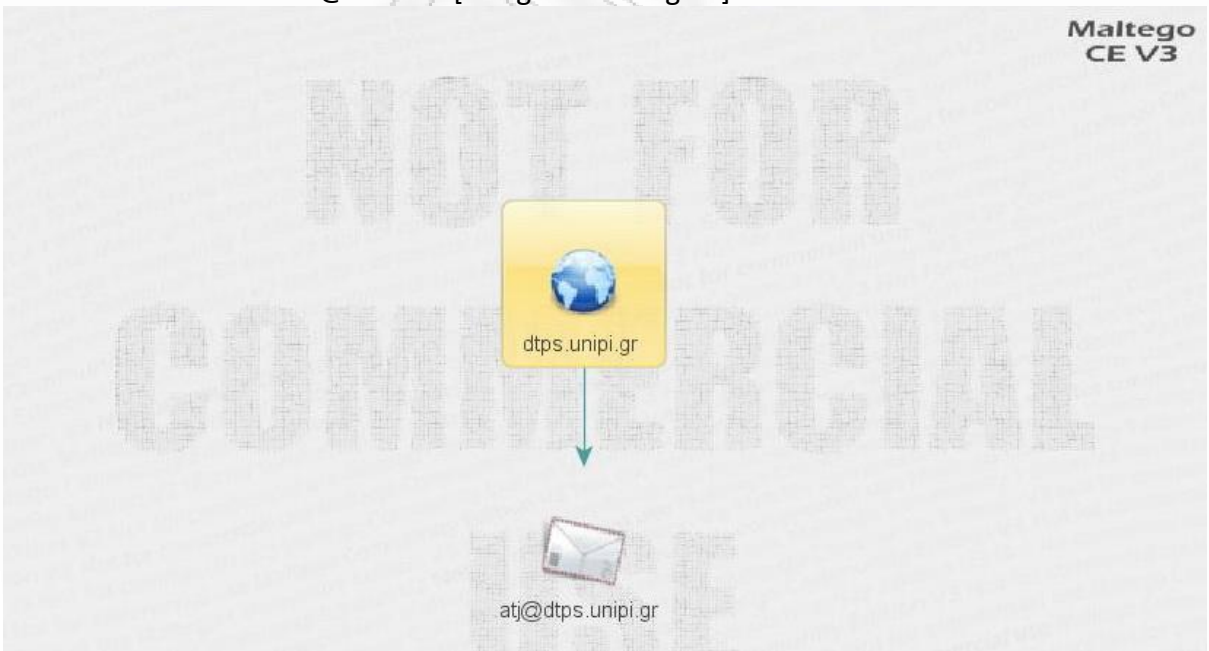


Transforms: To Domain
To Email Address
To Person [PGP]
To Phone Numbers

To Website



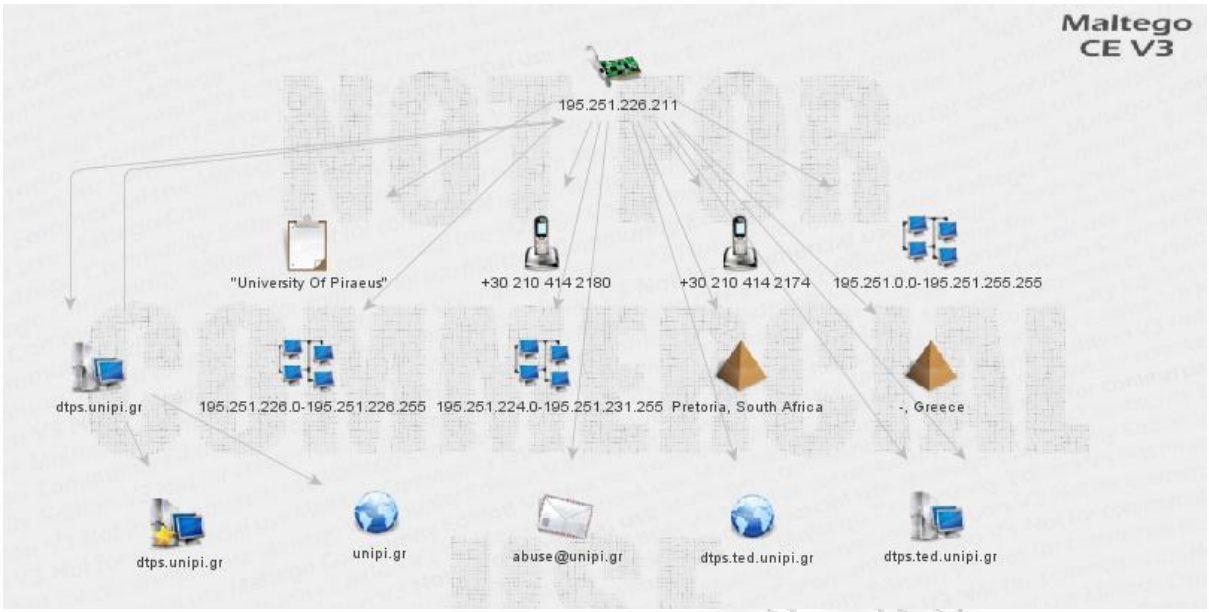
- https://dtps.unipi.gr
  - Email addresses from Domain
    -To Email addresses [From whois info]
    -To Email addresses [PGP]
    -To Email @domain [using Search Engine]



- DNS from Domain
  -To DNS Name – MX (mail server)
  -To DNS Name – NS (name server)
  -To DNS Name [Attempt zone transfer]

- To DNS Name [Find common DNS names]
-To DNS Name [Name Schema]
-To Website DNS [using Search Engine]
-To Website [Quick look up]

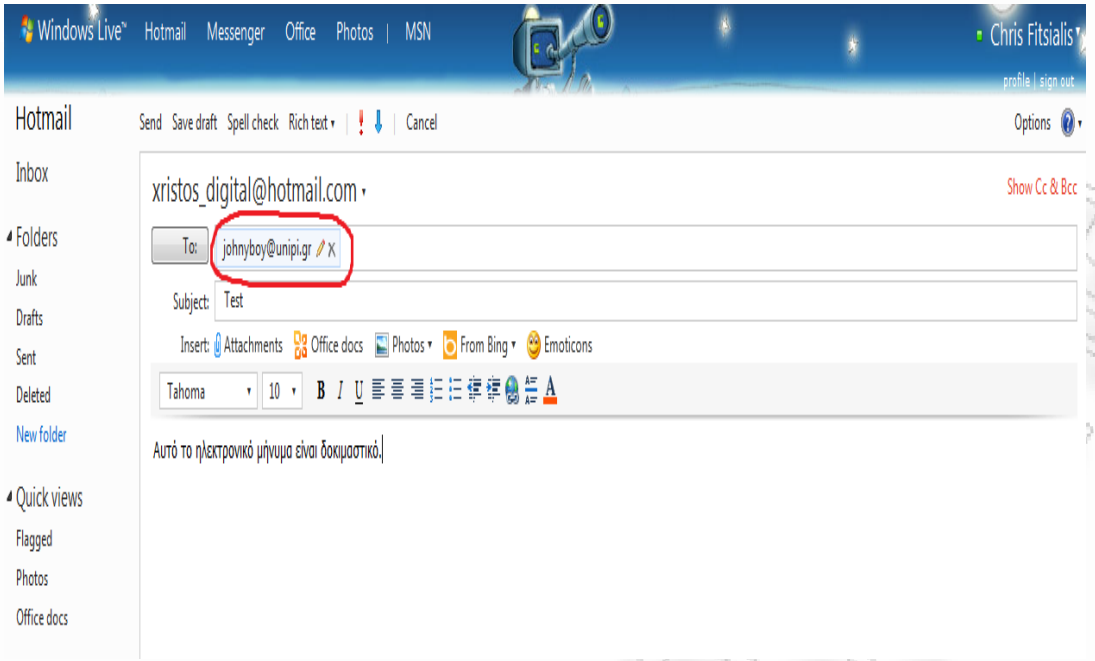
- Other transforms
  - To Domain [Find other TLDs]
  - To Email addresses [using Search Engine]
  - To Person [PGP]
  - To Phone Number [using Search Engine]
  - To Website [using Search Engine]



- Τεχνική SMTP Mail Bounce

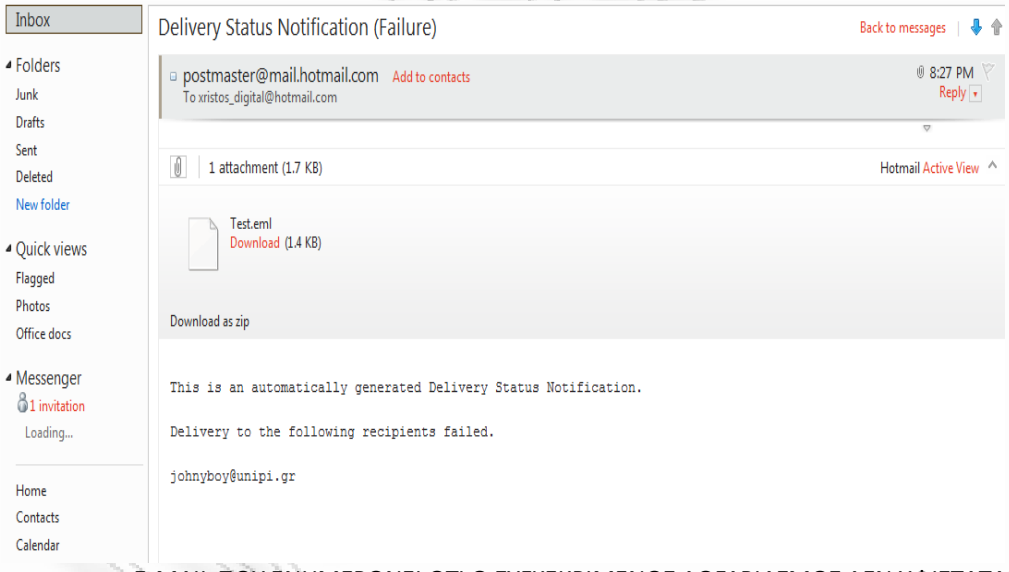
Εάν πολλές από τις μεθόδους που χρησιμοποιούνται αποτυγχάνουν, είναι πολύ εύκολο να εκτελεστεί μία πολυ εύκολη τεχνική η οποία ονομάζεται αναπήδηση ηλεκτρονικού μηνύματος. Αν και πολύ απλή αυτή η μέθοδος αξίζει το χρόνο που απαιτείται για να εκτελεστεί. Η βασική αρχή έχει να κάνει με τη αποστολή ενός απλού ηλεκτρονικού μηνύματος σε διεύθυνση η οποία βρίσκεται μέσα στο domain και η οποία υποθέτουμε ότι δεν υφίσταται. Ελπίζουμε έτσι ότι το μήνυμα θα βρει φθάσει τελικά στο πραγματικό mail server ο οποίος είναι υπεύθυνος για το domain, όπου και θα απορριφθεί και θα αποσταλεί πίσω σε εμάς. Με αυτό το τρόπο θα γίνει καταγραφή των ονομάτων συστημάτων και των IP διευθύνσεων των servers που διαχειρίζονται τη διαδικασία αυτή. Μαθαίνουμε έτσι πολλά για την υποδομή την οποία μελετάμε.

Στέλνουμε έτσι ένα ηλεκτρονικό μήνυμα στο domain unipi αλλά σε λογαριασμό ο οποίος υποθέτουμε ότι δεν υπάρχει και μελετάμε το μήνυμα που επιστράφηκε για τυχόν πληροφορίες οι οποίες καταγράφονται εκεί. Έχουμε λοιπόν:



Αποστολή e-mail στο domain unipi σε λογαριασμό που υποθέτουμε ότι δεν υπάρχει

Στη συνέχεια λαμβάνουμε από το mail server του πανεπιστημίου το παρακάτω απαντητικό e-mail το οποίο μας ενημερώνει ότι ο λογαριασμός johnyboy@unipi.gr δεν υφίσταται. Μελετάμε το συγκεκριμένο e-mail για τυχόν πληροφορίες τις οποίες μπορούμε να εκμαιεύσουμε.



Ε-MAIL ΠΟΥ ΕΝΗΜΕΡΩΝΕΙ ΟΤΙ Ο ΣΥΓΚΕΚΡΙΜΕΝΟΣ ΛΟΓΑΡΙΑΣΜΟΣ ΔΕΝ ΥΦΙΣΤΑΤΑΙ

Τέλος, μελετώντας το e-mail που λάβαμε δε είναι εφικτό να νακαλύχουμε περαιτέρω πληροφορία από αυτή που ήδη γνωρίζουμε. Δεν αποκαλύπτεται πληροφορία ούτε στο header του μηνύματος κάτι που μας οδηγεί στο συμπέρασμα ότι ο mail server του πανεπιστημίου είναι ρυθμισμένος να μην αποκαλύπτει πληροφορίες που αφορούν την πληροφοριακή υποδομή του πανεπιστημίου.

2 Ανάκτηση εγγραφών DNS από δημόσια διαθέσιμους διακομιστές

Περιλαμβάνει:

- Είδη καταγεγραμμένων πληροφοριών:

  - SOA Records - Δηλώνει το διακομιστή που έχει δικαιοδοσία για το domain.
  - MX Records - Κατάλογος των hosts ή του domain mail exchange server.
  - NS Records – Κατάλογος των hosts ή του domain name server.
  - A Records – Μια καταγραφή διεύθυνσης που επιτρέπει σε ένα όνομα υπολογιστή να μεταφραστεί σε μια IP διεύθυνση. Κάθε υπολογιστής οφείλει να έχει αυτή την καταγραφή για την δική του IP διεύθυνση που βρίσκεται μέσω του DNS.
  - PTR Records – Παραθέτει το domain name του host, ο host προσδιορίζεται από την IP διεύθυνσή του.
  - SRV Records – Καταγραφή της παρεχόμενης υπηρεσίας βάσει της τοποθεσίας (Service location record).
  - TXT Records – Γενικές καταγραφές κειμένου.
  - RP – Υπεύθυνο άτομο για το domain.

  - Sub Domains

Αποτελέσματα:

Μέσω του Central Ops (http://centralops.net/co/) όπως είδαμε και στον προηγούμενο βήμα έχουμε όσον αφορά τα DNS records, τα ακόλουθα αποτελέσματα:

- www.unipi.gr

DNS records

name	class	type	data	time to live
www.unipi.gr	IN	CNAME	spider.unipi.gr	500s (00:08:20)
spider.unipi.gr	IN	MX	preference: 5 exchange: webmail.unipi.gr	500s (00:08:20)
spider.unipi.gr	IN	A	195.251.229.6	500s (00:08:20)
unipi.gr	IN	SOA	server: ns.unipi.gr email: root.unipi.gr serial: 2011033101 refresh: 1200 retry: 7200 expire: 2419200 minimum ttl: 86400	500s (00:08:20)

unipi.gr	IN	MX	preference: 5 exchange: mailhost.unipi.gr	500s	(00:08:20)
unipi.gr	IN	NS	ns.unipi.gr	500s	(00:08:20)
unipi.gr	IN	NS	sns1.grnet.gr	500s	(00:08:20)
unipi.gr	IN	NS	sns0.grnet.gr	500s	(00:08:20)
6.229.251.195.in-addr.arpa	IN	PTR	spider.unipi.gr	86400s	(1.00:00:00)

- dtps.unipi.gr

DNS records

name	class	type	data	time to live	
dtps.unipi.gr	IN	CNAME	dtps.ted.unipi.gr	500s	(00:08:20)
dtps.ted.unipi.gr	IN	MX	preference: 5 exchange: dtps.ted.unipi.gr	500s	(00:08:20)
dtps.ted.unipi.gr	IN	A	195.251.226.211	500s	(00:08:20)
unipi.gr	IN	SOA	server: ns.unipi.gr email: root.unipi.gr serial: 2011033101 refresh: 1200 retry: 7200 expire: 2419200 minimum ttl: 86400	500s	(00:08:20)
unipi.gr	IN	NS	sns0.grnet.gr	500s	(00:08:20)
unipi.gr	IN	NS	sns1.grnet.gr	500s	(00:08:20)
unipi.gr	IN	NS	ns.unipi.gr	500s	(00:08:20)
unipi.gr	IN	MX	preference: 5 exchange: mailhost.unipi.gr	500s	(00:08:20)
211.226.251.195.in-addr.arpa	IN	PTR	dtps.ted.unipi.gr	86400s	(1.00:00:00)

Όσον αφορά τα **sub-domains** είναι η έξοδος που έβγαλε η ιστοσελίδα Robtex στο προηγούμενο βήμα.

3 Social Engineering

Μπορούμε να χωρίσουμε την διαδικασία του social engineering σε δύο φάσεις. Την φάση της συλλογής των στοιχείων των ατόμων που εργάζονται στην εταιρεία η οποία έχει το

πληροφοριακό σύστημα που μελετάμε και την φάση όπου κάνουμε μια ενεργή επίθεση στα άτομα των οποίων τα στοιχεία έχουμε λάβει από την προηγούμενη φάση.

Πρώτη φάση:
Τα άτομα-εργαζόμενοι τα στοιχεία των οποίων θέλουμε να συλλέγουμε στην πρώτη φάση είναι όλα εκείνα όσα έρχονται σε επαφή με το πληροφοριακό σύστημα είτε άμεση είτε έμμεση, είτε τοπικά είτε απομακρυσμένα. Με ιδιαίτερη προτίμηση σε αυτά που έχουν δικαιώματα πρόσβασης στο πληροφοριακό σύστημα αλλά και συγκεκριμένα σε εφαρμογές και δεδομένα που αυτό περιέχει.
Τα αποτελέσματα αρχικά θα πρέπει να είναι της μορφής:

- Όνομα
- Αριθμός Τηλεφώνου
- Email
- Νούμερο Γραφείου
- Τμήμα
- Ρόλος στην εταιρεία
- Επίπεδο γνώσεων στην πληροφορική και ασφάλεια

Έτσι ώστε να έχουμε συλλέξει τις απαραίτητες πληροφορίες για κάθε άτομο-στόχο ώστε να προχωρήσουμε στην επόμενη φάση με μεγαλύτερη ασφάλεια και επιτυχία.

Πηγές πληροφοριών:
Ανάλογα με το είδος του Οργανισμού που θέλουμε να εκτελέσουμε το Penetration Test εξαρτώνται και οι πηγές από όπου θα συλλέξουμε τα στοιχεία για να ολοκληρώσουμε την πρώτη φάση του social engineering. Συνήθως η κύρια πηγή πληροφοριών είναι το διαδίκτυο, όπου ξεκινώντας από την ιστοσελίδα του Οργανισμού μαθαίνουμε τα ονόματα της Διοίκησης καθώς και τα βασικά στοιχεία επικοινωνίας αυτών, όπως εσωτερικά τηλέφωνα και εταιρικούς λογαριασμούς e-mail. Στην συνέχεια προχωρούμε με τα ήδη υπάρχοντα στοιχεία που έχουμε πάνω σε κάποια συγκεκριμένα πρόσωπα να εμβαθύνουμε τις γνώσεις μας πάνω σε αυτά ανατρέχοντας είτε στην αναζήτηση σε κάποιες μηχανές αναζήτησης είτε σε κάποια κοινωνικά δίκτυα τα οποία είναι μέλη. Τέλος υπάρχει η δυνατότητα να τηλεφωνήσουμε στον Οργανισμό ερευνούμε και έχοντας κάποια στοιχεία για κάποιο εργαζόμενο να προσπαθήσουμε να συλλέξουμε περισσότερα ώστε να προχωρήσουμε στην επόμενη φάση. Τέλος μέσο αναζήτησης σε μηχανές αναζήτησης και σε κοινωνικά δίκτυα θέτοντας ως λήμμα στην αναζήτηση μας το όνομα του Οργανισμού μπορούμε να βρούμε και άλλους εργαζόμενους. Η αναζήτηση περεταίρω εργαζόμενων μπορεί να επιτευχθεί και μέσω των ατόμων που ήδη έχουμε εντοπίσει προηγουμένως στα κοινωνικά δίκτυα τα οποία έχουν συνδεθεί με κάποιους με εντοπισμένους εργαζόμενους.

Δεύτερη φάση:
Στην δεύτερη φάση όπως αναφέρθηκε και παραπάνω προχωρούμε σε μια ενεργή επίθεση στους εργαζόμενους των οποίων τα στοιχεία έχουμε συλλέξει στην πρώτη φάση. Επικεντρωνόμαστε σε άτομα που έχουν τόσο χαμηλή γνώση πάνω σε θέματα ασφάλειας πληροφοριακών συστημάτων, όσο και σε άτομα που έχουν αυξημένα δικαιώματα πρόσβασης και χρήσης της πληροφοριακής υποδομής, αλλά και σε άτομα που έχουν

δικαιώματα απομακρυσμένης πρόσβασης στο πληροφοριακό σύστημα είτε για απλή χρήση είτε για τη συντήρηση αυτού.

Η επίθεση:
Μέθοδοι
Οι μέθοδοι που έχουμε για μια επίθεση social engineering είναι οι ακόλουθοι:

Απομακρυσμένα:
E-mails: Αποστέλλουμε μηνύματα ηλεκτρονικού ταχυδρομείου στους εργαζόμενους που έχουμε επιλέξει τα οποία έχουν περιεχόμενο κατάλληλο, τέτοιο ώστε να πείσουν τον παραλήπτη να μας αποστείλει στοιχεία όπως το username και password με το οποίο συνδέεται στο σύστημα ή στο e-mail του, την δομή του πληροφοριακού συστήματος, συνήθη προβλήματα που έχει αυτό και γενικά ότι μπορεί να μας βοηθήσει σε έναν μεγάλο ή μικρό βαθμό για να μπορέσουμε χωρίς ιδιαίτερες τεχνικές μεθόδους να συνδεθούμε στο πληροφοριακό σύστημα. Αξίζει να σημειωθεί ότι το e-mail που αποστέλλουμε τα συγκεκριμένα μηνύματα πρέπει να πείθει τον παραλήπτη ότι ο αποστολέας έχει σχέση με την εταιρεία ή τις εταιρείες οι οποίες υποστηρίζουν το πληροφοριακό του Οργανισμού.
Τηλεφωνήματα: Γνωρίζοντας τα εσωτερικά ή και τα προσωπικά τηλέφωνα κάποιων εργαζομένων στον Οργανισμό μπορούμε να κάνουμε πιο άμεσα και γρήγορα ότι μπορούμε να κάνουμε με τα μηνύματα ηλεκτρονικού ταχυδρομείου. Αναφέρουμε ότι είναι δυνατό να λάβουμε αρκετές πληροφορίες τις οποίες δεν είναι δυνατό να λάβουμε μέσω των e-mail.

Τοπικά:
Επαφή: Προσποιούμενοι ότι είμαστε άτομα της εταιρείας υποστήριξης του πληροφοριακού συστήματος του Οργανισμού μπορούμε να έχουμε άμεση επαφή με άτομα που χρησιμοποιούν το πληροφοριακό σύστημα και να μάθουμε πολύ περισσότερες πληροφορίες, ενώ είναι δυνατό να παρακολουθήσουμε και τα πληκτρολόγια τους ενώ κάνουν σύνδεση στο σύστημα. Επίσης μέσω της προσωπικής επαφής έχουμε άμεση πρόσβαση σε κάποιο τερματικό του συστήματος στο οποίο ίσως είναι δυνατό να εκτελέσουμε κάποιο πρόγραμμα και να επιτεθούμε στην συνέχεια εκ των έσω. Απαραίτητη προϋπόθεση αποτελεί για την επιτυχία σε μεγάλο ή μικρό βαθμό αυτής της μεθόδου, να φανούμε πιστευτοί στους εργαζόμενους-χρήστες με τους οποίους θα έρθουμε σε επαφή. Αυτό μπορεί να επιτευχθεί έχοντας μαζί μας πλαστές εταιρικές κάρτες, να αναφέρουμε ότι είμαστε εκεί εκ μέρους κάποιου εργαζομένου που είναι αρμόδιος με το πληροφοριακό σύστημα, να έχουμε λογαριασμό e-mail με domain ίδιο με αυτό που χρησιμοποιεί η εταιρία υποστήριξης, κατάλληλη ενδυμασία κλπ.
Συντονισμός

Για την επιτυχία των παραπάνω επιθέσεων εκτός από την σύνταξη του κατάλληλου μηνύματος ηλεκτρονικού ταχυδρομείου, της κατάλληλης συζήτησης στο τηλέφωνο καθώς και της άρτιας διαδικαστικά φυσικής επαφής παίζει τεράστιο ρόλο και ο συντονισμός της χρήσης της κάθε μεθόδου και των μέσων της.

Ο **συντονισμός** περιλαμβάνει:
Την άρτια οργάνωση και αποστολή των e-mail την κατάλληλη ώρα και μέρα. Όπου θα πρέπει να αποσταλούν πρώτα στους χρήστες με χαμηλή γνώση πάνω στην ασφάλεια και

στην συνέχεια σε αυτούς με μέτρια, εργάσιμες ώρες και σχετικά νωρίς. Κατά προτίμηση πριν την ώρα που φτάνει στο κτήριο του οργανισμού ο υπεύθυνος μηχανοργάνωσης.
Μετά την αποστολή των e-mail θα πρέπει να προχωρήσουμε άμεσα στα τηλεφωνήματα, στους χρήστες στους οποίους αποστείλαμε τα e-mail (εφόσον θέλουμε να χρησιμοποιήσουμε και αυτό το μέσο), έτσι ώστε να τους πείσουμε περισσότερο για την ταυτότητα μας, και να τους πιάσουμε περισσότερο απροετοίμαστους ώστε να τους ξεφύγουν περισσότερες πληροφορίες. Σε περίπτωση που έχουμε τα προσωπικά κινητά των εργαζομένων και ξέρουμε ότι έχουν λάβει το e-mail που στείλαμε και βρίσκονται στο

Είναι δυνατό να πραγματοποιήσουμε μόνο μία μέθοδο από τις δύο καθώς και να γίνει μόνο η χρήση ενός μέσου.

Στοιχεία:

Όνομα	Ρόλος	Γραφείο	Τηλέφωνο	E-mail
Αβραντινής Νικόλαος	ΙΔΑΧ ΠΕ Πληροφορικής, Υπάλληλος : Τμ. Μηχανοργάνωσης	ΚΕΚΤ/11	210 414 2408	avrad@unipi.gr
Αγγελοπούλου Σταματίνα	Υπάλληλος : Γραφείο Προέδρου Τμήματος Οικονομικής Επιστήμης	ΚΕΚΤ/532	210 414 2300	saggel@unipi.gr
Αγιακλόγλου Χρήστος	Καθηγητής Τμήμα Οικονομικής Επιστήμης	ΚΕΚΤ/523	210 414 2290	agiaklis@unipi.gr
Αλεξάκης Χρήστος	Επίκουρος Καθηγητής Τμήμα Οικονομικής Επιστήμης	ΚΕΚΤ/501	210 414 2337	alexakis@unipi.gr
Αλεξανδρή Ευφροσύνη	Μόνιμο Προσωπικό ΔΕ Διοικ.-Λογ., Γραμματεία Ναυτιλιακών Σπουδών	ΚΕΚΤ/113	210 414 2175	
Αλεξανδρής Νικόλαος	Καθηγητής Τμήμα Πληροφορικής	ΚΕΚΤ/504	210 414 2267	alexandr@unipi.gr
Αλεξιάδου - Κοτίου Ελπίδα	ΕΕΔΙΠ Τμήμα Διεθνών Και Ευρωπαικών Σπουδών	ΚΕΚΤ/322	210 414 2176	ealexi@unipi.gr
Αλεξίου Αγγελική	Επίκουρος Καθηγητής Τμήμα Ψηφιακών Συστημάτων	ΑΝΔΡ/303	210 414 2761	alexiou@unipi.gr
Αληγεωργίου Κων/νος	Μόνιμο Προσωπικό ΤΕ Μηχανικών, Υπάλληλος : Τμ. Τεχνικών Έργων	ΚΕΚΤ/117	210 414 2069	aliko@unipi.gr
Αλμπάνη Σουλτάνα	ΙΔΑΧ ΤΕ Βιβλ/μων, Υπάλληλος : Βιβλιοθήκη	ΚΕΚΤ/ΥΟ7	210 414 2036	talbani@unipi.gr
Ανδριόπουλος Φαίδω	Βοηθός Τμήμα Οικονομικής Επιστήμης	ΚΕΚΤ/520	210 414 2025	fandri@unipi.gr
Αντζουλάκος Δημήτριος	Αναπληρωτής Καθηγητής Τμήμα Στατιστικής Και Ασφαλιστικής Επιστήμης	ΚΕΚΤ/307	210 414 2388	dantz@unipi.gr
Αντζουλάτος Άγγελος	Καθηγητής Τμήμα Χρηματοοικονομικής Και Τραπεζικής Διοικητικής	ΚΕΚΤ/330	210 414 2185	antzoul@unipi.gr
Αντωνίου Παρασκευή	Μόνιμο Προσωπικό ΔΕ Διοικ.-Λογ., Προϊστάμενος/η : Γραμματεία Τμήματος Ψηφιακών Συστημάτων		210 414 2235	panton@unipi.gr
Απέργης Νικόλαος	Καθηγητής, Πρόεδρος Τμήματος : Τμήμα Χρηματοοικονομικής Και Τραπεζικής Διοικητικής	ΚΕΚΤ/329	210 414 2429	napergis@unipi.gr
Αποστόλου	Επίκουρος Καθηγητής Τμήμα	ΓΛ126/30	210 414 2476	dapost@unipi.gr

Δημήτριος	Πληροφορικής	3		
Αποστόλου Ευαγγελία	ΕΤΕΠ ΠΕ, Υπάλληλος : Γραφείο Προέδρου Τμήματος Χρηματοοικονομικής Και Τραπεζικής Διοικητικής	ΚΕΚΤ/328	210 414 2183	lapost@unipi.gr
Αρτέμη Διονυσία	ΙΔΑΧ ΠΕ Διοικ.-Οικ., Υπάλληλος : Προϊστάμενος Γραμματείας	ΚΕΚΤ/419	210 414 2229	dionysia@unipi.gr
Αρτίκης Θεόδωρος	Καθηγητής Τμήμα Στατιστικής Και Ασφαλιστικής Επιστήμης	ΚΕΚΤ/539	210 414 2310	artik@unipi.gr
Αρτίκης Παναγιώτης	Επίκουρος Καθηγητής Τμήμα Οργάνωσης Και Διοίκησης Επιχειρήσεων	ΚΕΚΤ/401	210 414 2200	partikis@unipi.gr
Ασδεράκη Φωτεινή	Λέκτορας Τμήμα Διεθνών Και Ευρωπαικών Σπουδών	ΑΝΔΡ/101	210 414 2713	asderaki@unipi.gr
Ασημακόπουλος Νικήτας	Καθηγητής Τμήμα Πληροφορικής	ΚΕΚΤ/308	210 414 2145	assinik@unipi.gr
Αυδάλα Σοφία	ΕΤΕΠ ΔΕ, Υπάλληλος : Γραμματεία Τμήματος Ναυτιλιακών Σπουδών	ΚΕΚΤ/113	210 414 2075	savdala@unipi.gr
Βαλμά Ερασμία	Λέκτορας Τμήμα Ναυτιλιακών Σπουδών	ΚΔ40/Β109	210 414 2512	valma@unipi.gr
Βαρελά Αδαμαντία	Μόνιμο Προσωπικό ΔΕ Προσ. Η/Υ, Υπάλληλος : Γραμματεία Τμήματος Οικονομικής Επιστήμης	ΚΕΚΤ/114	210 414 2081	avarela@unipi.gr
Βαρέλη Αικατερίνη	ΙΔΑΧ ΔΕ Διοικ.-Λογ., Υπάλληλος : Γραφείο Πρυτάνεων Και Αντιπρυτάνεων		210 414 2411	kvareli@unipi.gr
Βασιλακόπουλος Γεώργιος	Καθηγητής, Αντιπρύτανης Ακαδημαικών Υποθέσεων & Προσωπικού : Πρυτανεία, Πρόεδρος Τμήματος : Τμήμα Ψηφιακών Συστημάτων	ΚΕΚΤ/309	210 414 2370	gvass@unipi.gr
Βασιλειάδου Καλλιόπη	Μόνιμο Προσωπικό ΠΕ Διοικ.-Οικ., Προϊστάμενος/η : Διεύθυνση Υποστήριξης Πανεπιστημιακών Οργάνων	ΚΕΚΤ/415	210 414 2224	pvas@unipi.gr
Βεζυρτζόγλου Ευπραξία	Μόνιμο Προσωπικό ΔΕ Διοικ.-Λογ., Προϊστάμενος/η : Γραμματεία Τμήματος Χρηματοοικονομικής Και Τραπεζικής Διοικητικής	ΚΕΚΤ/109	210 414 2364	efivez@unipi.gr
Βελκοπούλου Αικατερίνη	ΙΔΑΧ ΔΕ Διοικ.-Λογ., Υπάλληλος : Γραμματεία Συγκλήτου Και Πρυτανικού Συμβουλίου	ΚΕΚΤ/416	210 414 2439	kvelko@unipi.gr
Βέργαδος Δημήτριος	Λέκτορας Τμήμα Πληροφορικής	ΓΛ126/301	210 414 2479	vergados@unipi.gr
Βερροπούλου Γεωργία	Επίκουρος Καθηγητής Τμήμα Στατιστικής Και Ασφαλιστικής Επιστήμης	ΓΛ126/601	210 414 2729	gverrop@unipi.gr
Βίρβου Μαρία	Καθηγητής Τμήμα Πληροφορικής	ΚΕΚΤ/507	210 414 2269	mvirvou@unipi.gr
Βλάχος Γεώργιος	Καθηγητής Τμήμα Ναυτιλιακών Σπουδών	ΚΔ40/Β303	210 414 2520	gvl@unipi.gr

Βοζίκης Αθανάσιος	Λέκτορας Τμήμα Οικονομικής Επιστήμης	ΚΕΚΤ/515	210 414 2280	avozik@unipi.gr
Βολιώτης Δημήτριος	Λέκτορας Τμήμα Χρηματοοικονομικής Και Τραπεζικής Διοικητικής	ΚΕΚΤ/331	210 414 2227	dvoliotis@unipi.gr
Βουγιουκλίδου Άννα	Λέκτορας Τμήμα Πληροφορικής	ΚΕΚΤ/322	210 414 2176	avou@unipi.gr
Βουδούρη Άννα	ΕΤΕΠ ΔΕ, Υπάλληλος : Τμήμα Φοιτητικής Μέριμνας	ΚΕΚΤ/116	210 414 2096	annavoud@unipi.gr
Βουδούρης Δημήτριος	Επιστημονικός Συνεργάτης Τμήμα Οικονομικής Επιστήμης	ΚΕΚΤ/520	210 414 2286	dvoud@unipi.gr
Βούδρης Χρήστος	Προϊστάμενος: Γραμματεία Συγκλήτου Πρυτανικού Συμβουλίου	ΚΕΚΤ/417	210 414 2238	cvoudris@unipi.gr
Βρόντος Σπυρίδων	Λέκτορας Τμήμα Στατιστικής Και Ασφαλιστικής Επιστήμης	ΓΛ126/404	210 414 2109	svrontos@unipi.gr
Γαλάνη Αρίστη	ΕΤΕΠ ΠΕ, Υπάλληλος : Κέντρο Διαχείρισης Δικτύων	ΚΕΚΤ/321	210 414 2172	agalani@unipi.gr
Γαραντζιώτη Γεωργία	ΙΔΑΧ ΠΕ Διοικ.-Οικ., Υπάλληλος : Γραμματεία Τμήματος Βιομηχανικής Διοίκησης Και Τεχνολογίας	ΚΕΚΤ/110	210 414 2098	ggarantz@unipi.gr
Γεροντή Αγγελική	ΕΕΔΙΠ Χωρίς Τμήμα		210 414 2351	ageron@unipi.gr
Γεωργακέλλος Δημήτριος	Αναπληρωτής Καθηγητής Τμήμα Οργάνωσης Και Διοίκησης Επιχειρήσεων	ΚΕΚΤ/434	210 414 2252	dgeorg@unipi.gr

Παράδειγμα:
Παράδειγμα απομακρυσμένης επίθεσης social engineering μέσω αποστολής e-mail για την απόκτηση στοιχείων όπως username password, αλλά και με σκοπό την προετοιμασία μια τοπικής επίθεσης social engineering στα γραφεία του πανεπιστημίου.

Σενάριο 1:
Γεια σας από σήμερα πραγματοποιούμε έναν έλεγχο στον Active Directory του Πανεπιστημίου και απαιτείται ο εκ νέου συγχρονισμός κάποιων λογαριασμών που βρίσκονται σε εκκρεμότητα για λογαριασμό του γραφείου μηχανοργάνωσης του Πανεπιστημίου Πειραιά. Παρακαλώ απαντήστε γράφοντας το όνομα χρήστη (username) και τον κωδικό πρόσβασης (password) που χρησιμοποιείτε για να συνδεθείτε στον υπολογιστή σας, μέχρι και σήμερα. Έχουμε επικοινωνήσει με τον κύριο Βασιλακόπουλο και τον κύριο Χρήστο Τάδε (υπεύθυνος Ασφάλειας γραφείου μηχανοργάνωσης) και έχει εγκρίνει αυτή τη διαδικασία. Στην συνέχεια θα συμπληρώσω τη βάση δεδομένων με τα στοιχεία του λογαριασμού σας, ώστε να είναι έτοιμα για να τα επανασυγχρονίσουμε με τον Active Directory με σκοπό η λειτουργία του λογαριασμού σας να αποκατασταθεί (αυτή η διαδικασία είναι διαφανής στον χρήστη και δεν χρειάζεται περαιτέρω ενέργειες από εσάς). Σκοπός αυτής της διαδικασίας είναι να μειωθεί ο χρόνος που απαιτείται από ορισμένους χρήστες για να συνδεθούν με το δίκτυο του Πανεπιστημίου

Με εκτίμηση
Υπεύθυνος Γραφείου Μηχανοργάνωσης.

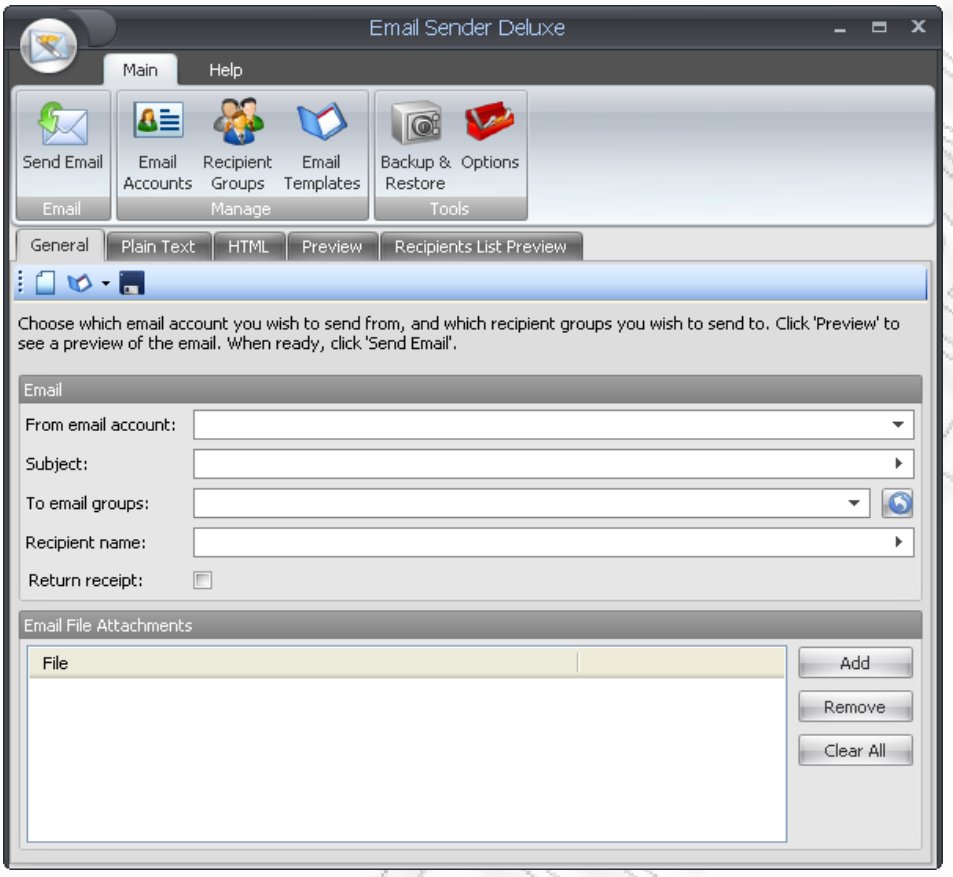
Σενάριο 2:
Καλημέρα
Το γραφείο Μηχανοργάνωσης είχε μια κρίσιμη αποτυχία εχθές το βράδυ σχετικά με την απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο του Πανεπιστημίου. Αυτό θα επηρεάσει μόνο τους χρήστες που περιστασιακά εργάζονται από το σπίτι. Αν έχετε απομακρυσμένη πρόσβαση, παρακαλώ στείλτε μου με το username σας και τα στοιχεία πρόσβασης σας π.χ πιο σύστημα απομακρυσμένης πρόσβασης χρησιμοποιήσατε; VPN και IP διεύθυνση κλπ και θα επαναφέρουμε το σύστημα. Επίσης υπάρχει η δυνατότητα με αυτή την ευκαιρία να αυξήσουμε τους χρήστες που έχουν απομακρυσμένη πρόσβαση, οπότε εάν πιστεύεται ότι χρειάζεστε να εργάζεστε από το σπίτι περιστασιακά, παρακαλώ στείλτε μου το όνομα χρήστη σας, ώστε να μπορέσουμε να τα προσθέσουμε στα σωστά groups. Εάν θέλετε να διατηρήσετε τα τρέχοντα διαπιστευτήρια σας, να στείλετε επίσης και τον κωδικό πρόσβασής σας. Δεν απαιτείται ο κωδικός πρόσβασης για την εκτέλεση της συντήρησης, αλλά αυτός θα αλλάξει αν δεν μας ενημερώσετε ποιος είναι αυτός. Ζητούμε συγγνώμη για την ταλαιπωρία που προκάλεσε το συγκεκριμένο γεγονός και εργαζόμαστε για την επίλυσή του το συντομότερο δυνατό.

Σας ευχαριστώ για την υπομονή και την βοήθειά σας.

Με σεβασμό
Υπεύθυνος Γραφείου Μηχανοργάνωσης.

Εργαλείο που χρησιμοποιήθηκε:

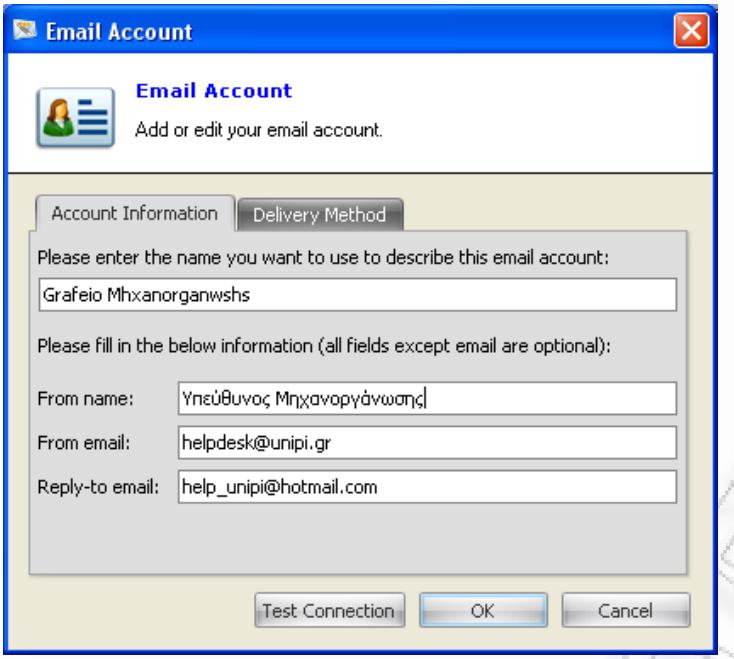
E-mail Sender Deluxe



Με το συγκεκριμένο εργαλείο μπορούμε να στείλουμε e-mails, τα οποία θα εμφανίζουν στον παραλήπτη όποια διεύθυνση e-mail και όνομα χρήστη εμείς θέλουμε.

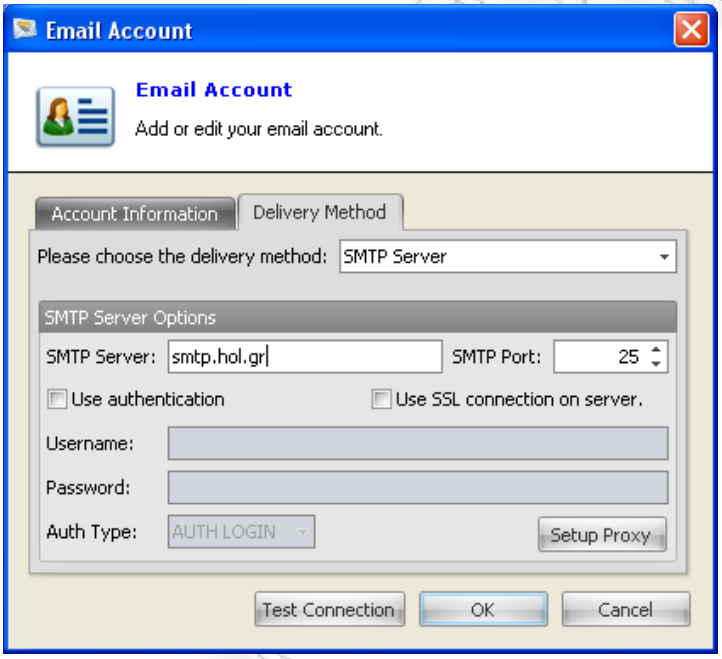
Ρυθμίζουμε αρχικά το όνομα χρήστη που θέλουμε να εμφανίζεται στα εισερχόμενα καθώς και το e-mail.

Βάζουμε ως όνομα Υπεύθυνος Μηχανοργάνωσης, e-mail helpdesk@unipi.gr και το e-mail που θα γίνεται forward η απάντηση το help_unipi@hotmail.com, όπως βλέπουμε παρακάτω:



Τέλος ρυθμίζουμε την μέθοδο παράδοσης (deliver method):

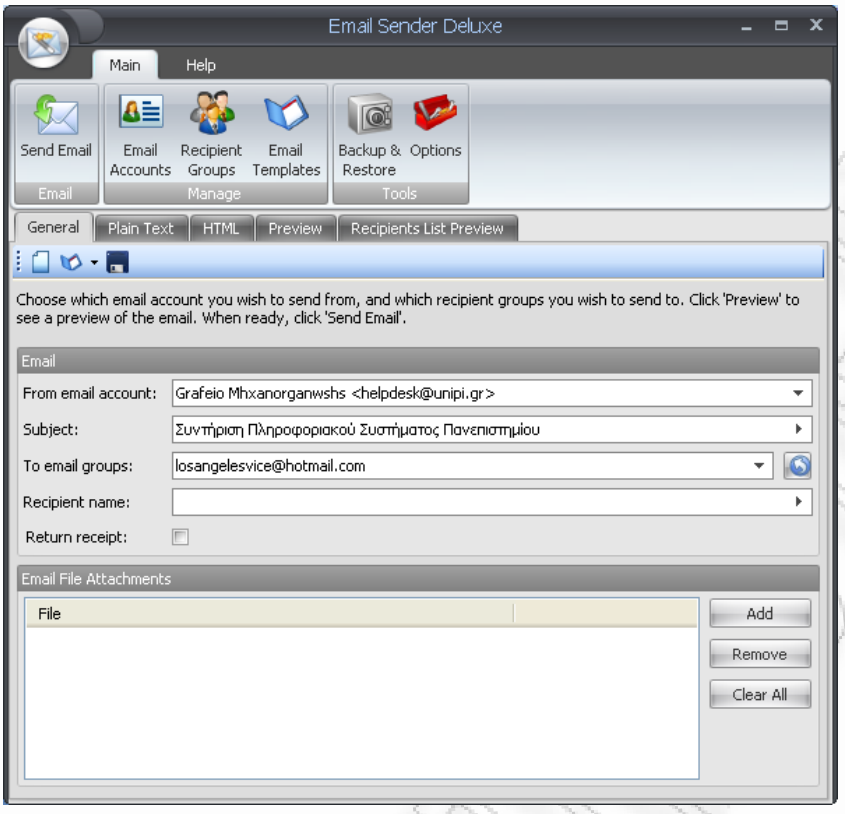
Στο συγκεκριμένο παράδειγμα απαιτείται μόνο η ρύθμιση του SMTP server που θα χρησιμοποιήσουμε ώστε να στείλουμε τα e-mails. Αξίζει να σημειωθεί ότι ο smtp server που δηλώνουμε, εφόσον δεν επιλέξουμε το use authentication, είναι ο default smtp server του internet service provider μας.



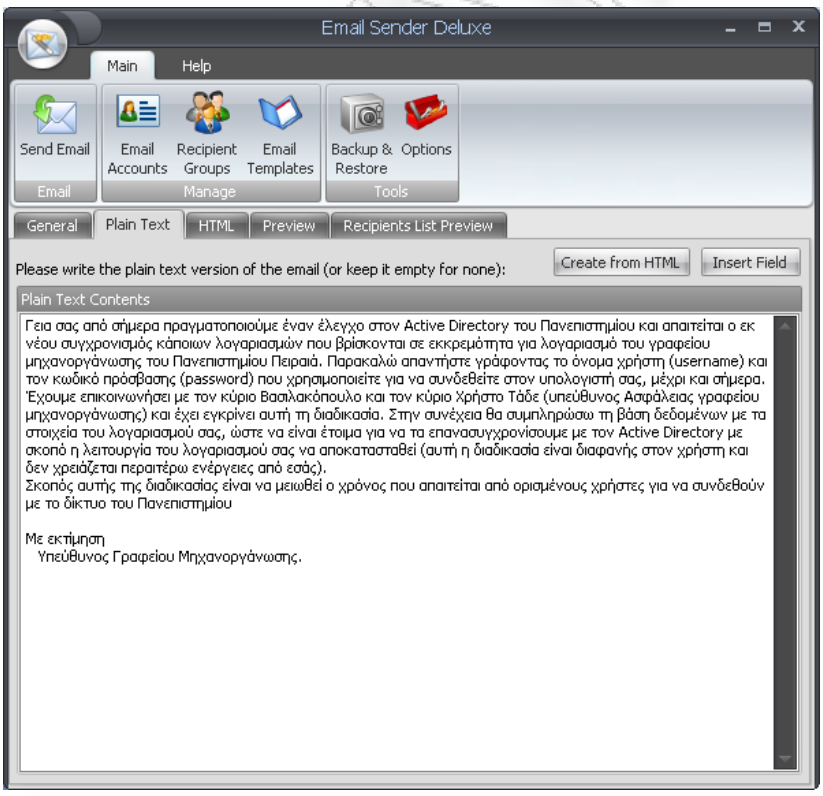
Κάνουμε κλικ στο Test Connection και αν όλα έχουν ρυθμιστεί σωστά παίρνουμε σχετικό μήνυμα.

Έτσι προχωρούμε στην αποστολή του e-mail του Σεναρίου 1, σε κάποιο χρήστη του πληροφοριακού συστήματος που έχουμε βρει από τα προηγούμενα βήματα.

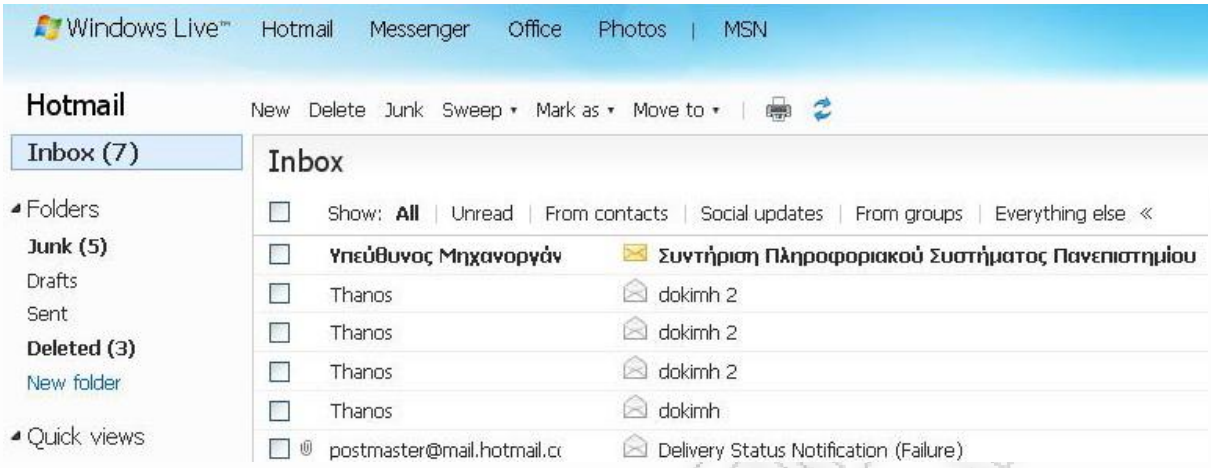
Βλέπουμε παρακάτω τον λογαριασμό e-mail από τον οποίο θα αποσταλεί το e-mail που θέλουμε να στείλουμε, τον τίτλο του e-mail, Συντήρηση Πληροφοριακού Συστήματος του Πανεπιστημίου, καθώς επίσης και τους λογαριασμούς e-mail στόχους που θα το στείλουμε.



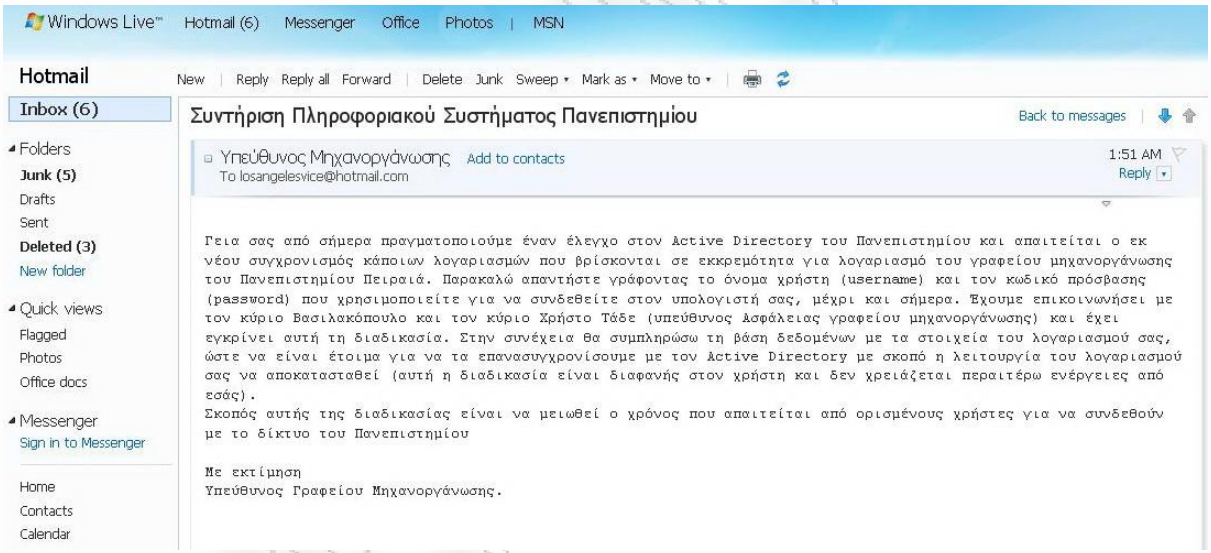
Τέλος προσθέτουμε το κείμενο που θέλουμε να στείλουμε μαζί με το e-mail.



Ελέγχουμε τα εισερχόμενα e-mail μας και βλέπουμε ότι το έχουμε λάβει.



Επίσης ανοίγουμε το συγκεκριμένο e-mail και βλέπουμε ότι έχει αποσταλεί το περιεχόμενο του Σεναρίου 1.



4. Dumpster Diving

Είναι η πρακτική κατά την οποία ψάχνουμε γενικά σε εμπορικούς ή οικιακούς κάδους σκουπιδιών για να βρούμε στοιχεία που έχουν απορριφθεί από τους ιδιοκτήτες τους, αλλά που μπορεί να είναι χρήσιμο αυτών που τα ψάχνει και ερευνά (dumpster diver).
Έτσι είναι δυνατό εντός των σκουπιδιών να βρούμε:

- Χαρτιά με username και passwords χρηστών
- Χαρτιά με διάφορα στοιχεία χρηστών
- Χαρτιά και σημειώσεις από το γραφείο μηχανοργάνωσης τα οποία θα παρέχουν πληροφορίες όσων αφορά το πληροφοριακό σύστημα που μελετάμε
- Χαρτιά με στοιχεία για συμβόλαια
- Παλιούς σκληρούς δίσκους, CD κλπ.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

- HACKING EXPOSED 6 NETWORK SECURITY SECRETS & SOLUTIONS 2009, Stuart McClure , Joel Scambray , George Kurtz

- PENETRATION TESTER'S OPEN SOURCE TOOLKIT VOLUME 2 2007, Aaron W. Bayles, Keith Butler, Adair John Collins, Haroon Meer, Eoin Miller, Gareth Murray Phillips, Michael J. Schearer, Jesse Varsalone, Thomas Wilhelm, Mark Wolfgang

- PROFESSIONAL PENETRATION TESTING CREATING AND OPERATING A FORMAL HACKING LAB 2010, Thomas Wilhelm

ΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

- www.vulnerabilityassessment.co.uk

- http://packetstormsecurity.org/

- http://www.securityfocus.com/