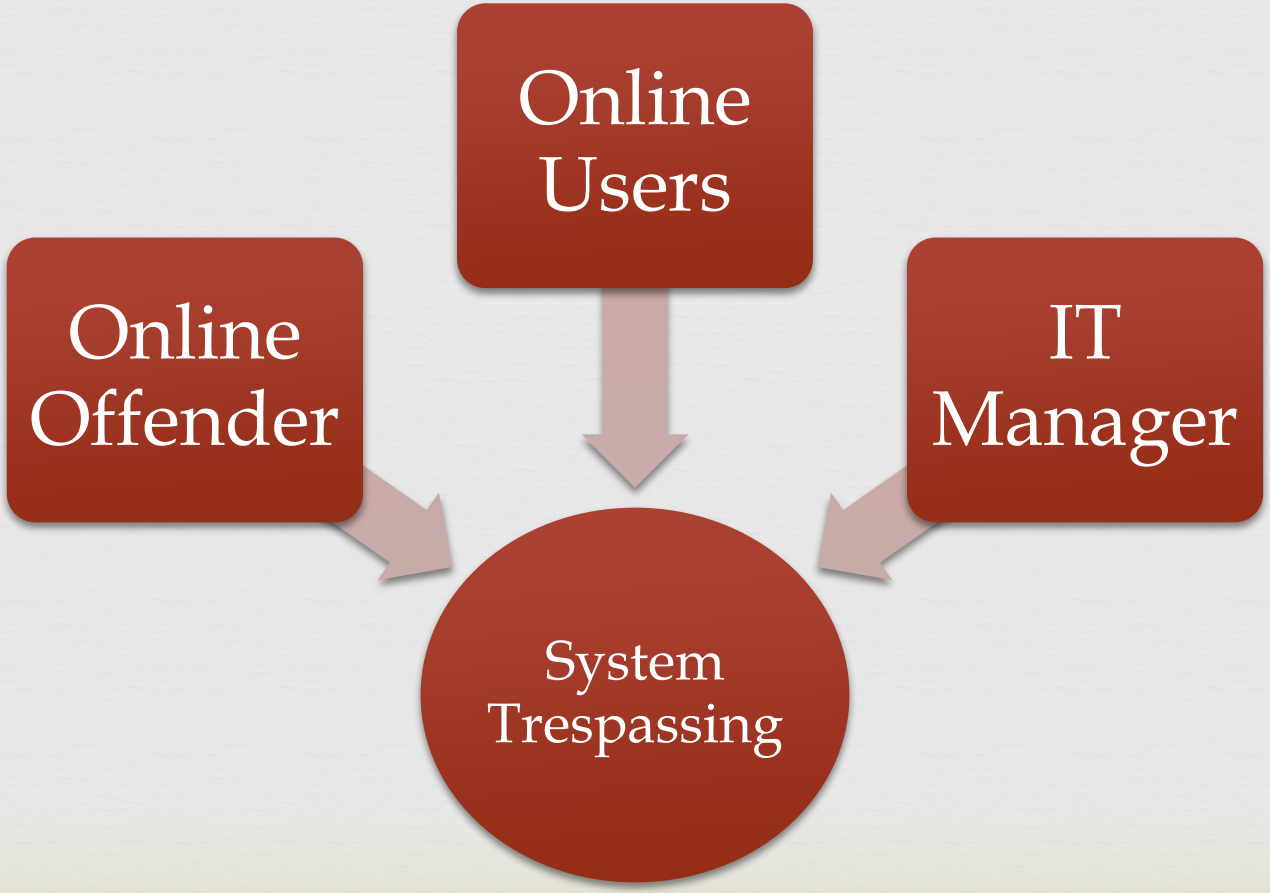
Evidence-Based Cyber Security: Suggestions and Recommendations for Building Cyber Resiliency Against System Trespassing Events

Dr. David Maimon
Associate Professor
Department of Criminology and Criminal Justice
Institute for Advanced Computer Science
University of Maryland

The Human Players



Outline

- System trespassing
- Deterrence in cyberspace
- Findings from 4 field experiments
- Social sciences and its relevance for strengthening the resilience of computing environments

David Maimon

System Trespassing Project

Michel

Bertrand

Teddy

Liz

Marial

Alex

The research team has been supported by grants from the “National Security Agency” and the “National Science Foundation”


I'm not a
Hacker
I'm a
"SECURITY
PROFESSIONAL"

Policy and Prior Research

- "Computer Fraud and Abuse Act" 1986
- National Institute of Standard and Technology (NIST controls)

National Institute of Standards and Technology
U.S. Department of Commerce

Evidence Based Policy

- Stresses moving beyond decision makers' political, financial, social background and personal experience to a model in which policy decision are made based on scientific studies findings.

Policy and Prior Research

- "Computer Fraud and Abuse Act" 1986
- National Institute of Standard and Technology (NIST controls)
- Prior research focuses mainly on the technical aspects of computer focused crimes

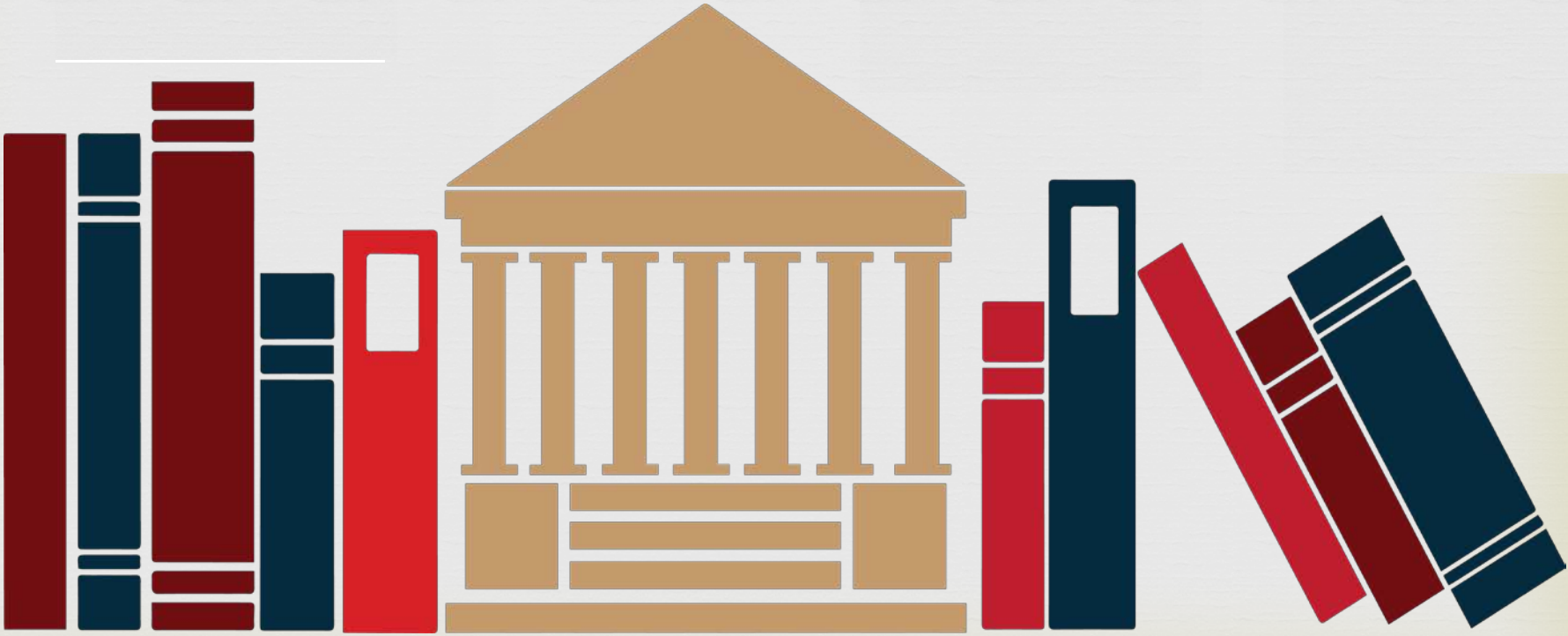
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Data on System Trespassing

Fortress vs. Bazaar Computing Environment

Computer environments in which substantial efforts are placed over access control and protection against external attacks

Bazaar Computer Environment



Honeypots

- A security resource whose value lies in being probed, attacked or compromised

Deterrence Theory

- Deterrence occurs when someone refrains from committing a crime because he/she fears the certainty, swiftness, and/ or severity of formal legal punishments

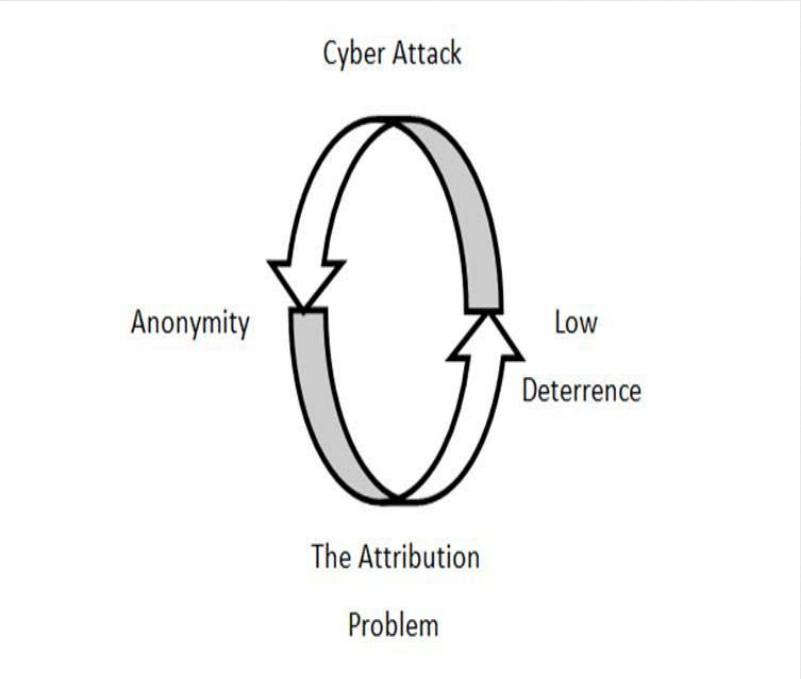
Absolute and Restrictive Deterrence (Gibbs 1975)

Absolute deterrence

Restrictive deterrence

Could Deterrence Really Work in Cyberspace?

NO !



Study 1: Goals

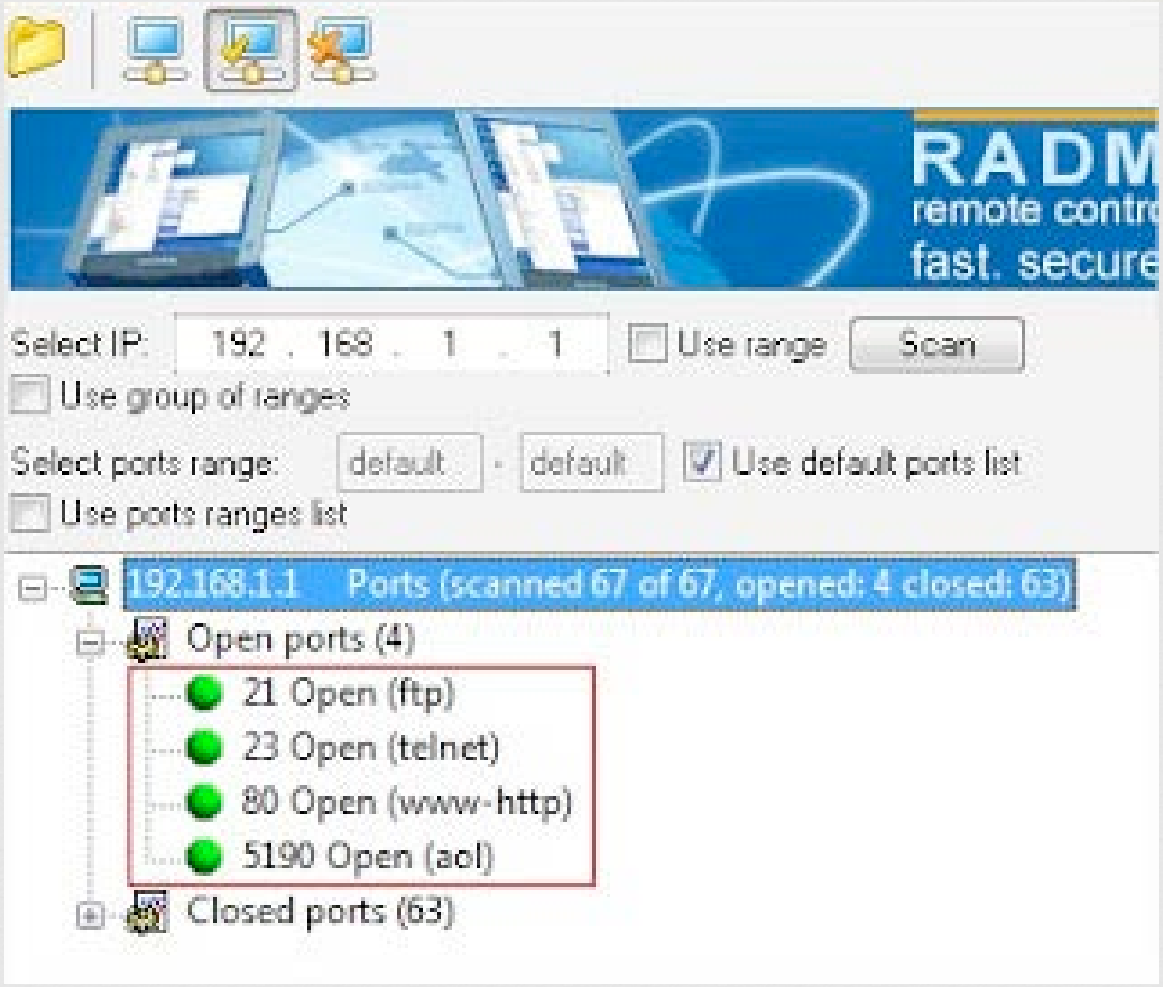
- Does a warning banner shape the development and progress of system trespassing incidents?
  - Immediate termination of trespassing incident
  - Frequency of repeated system trespassing incidentss
  - Duration of system trespassing incidents

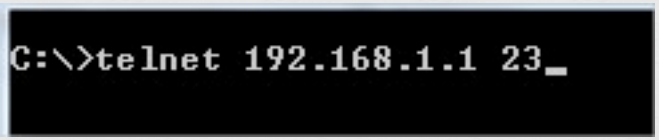
Experiment #1: Design

- 80 public IP addresses
- Experimental period: 2 months
- Waited…..
- Simulated a genuine environment

Gaining Access to the Target Computers

Scan




C:\>telnet 192.168.1.1 23


Login: admin
Password:

Gaining Access to the Target Computers

Scan

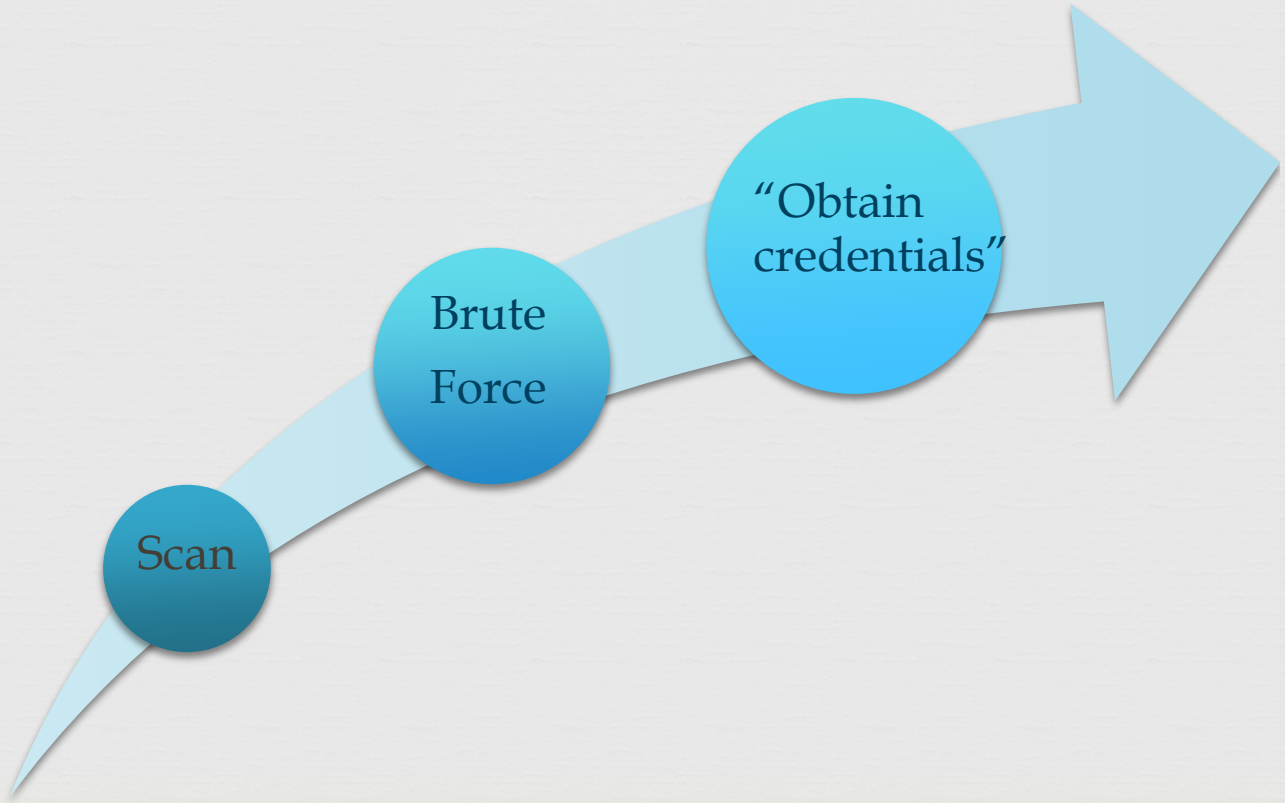
Brute Force

root@bt: /pentest/passwords/cwf

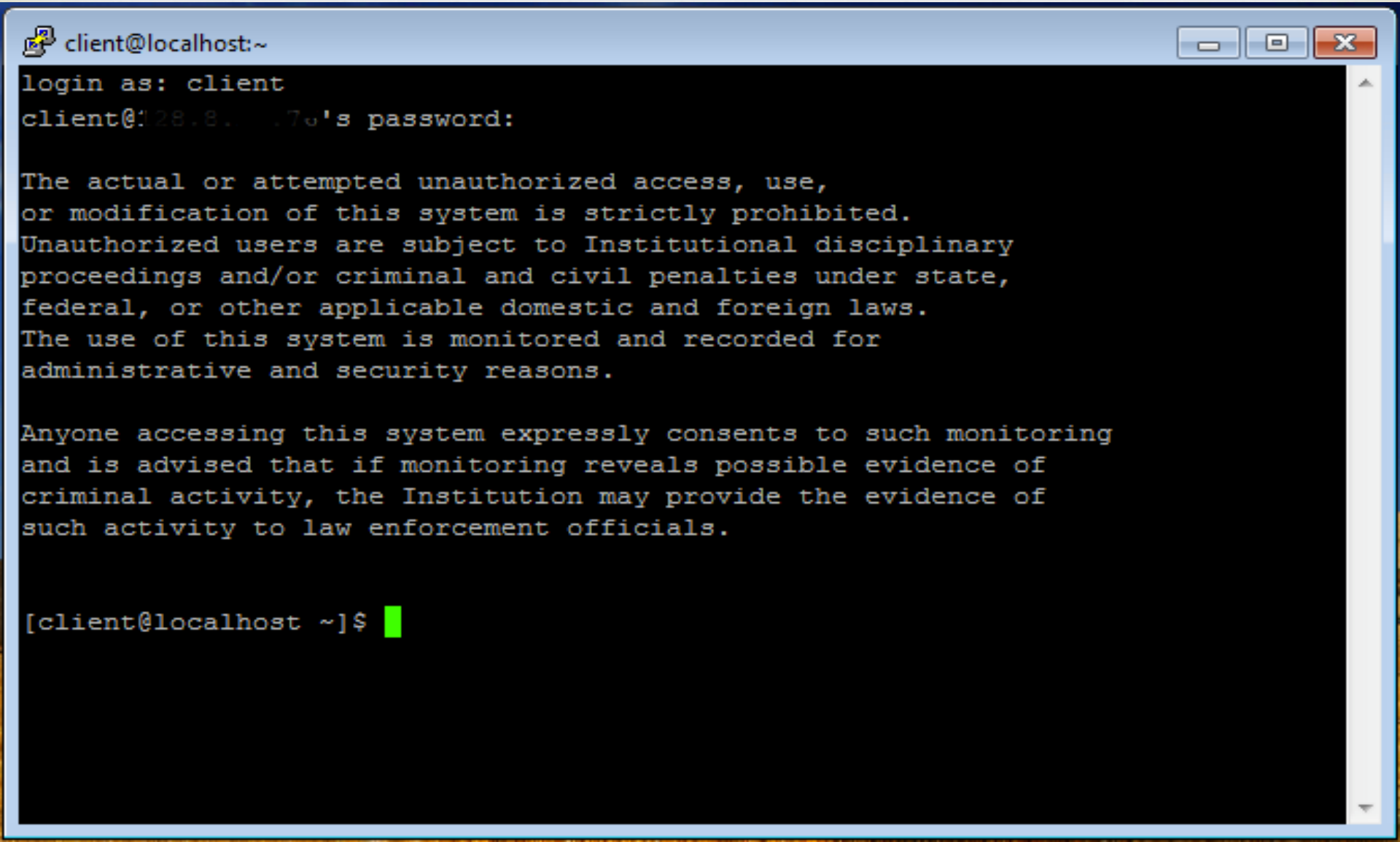
File Edit View Terminal Help

```
#####################################################
#                    Crack Web Form                 #
#####################################################
[Attempt]: 0 [Username]: admin [Password]: 0 [Status]: Failed
[Attempt]: 1 [Username]: admin [Password]: 0000 [Status]: Failed
[Attempt]: 2 [Username]: admin [Password]: 00000000 [Status]: Failed
[Attempt]: 3 [Username]: admin [Password]: 0000010023 [Status]: Failed
[Attempt]: 4 [Username]: admin [Password]: 1064 [Status]: Failed
[Attempt]: 5 [Username]: admin [Password]: 1111 [Status]: Failed
[Attempt]: 6 [Username]: admin [Password]: 123 [Status]: Failed
[Attempt]: 7 [Username]: admin [Password]: 1234 [Status]: Failed
[Attempt]: 8 [Username]: admin [Password]: 12345 [Status]: Failed
[Attempt]: 9 [Username]: admin [Password]: 123456 [Status]: Failed
[Attempt]: 10 [Username]: admin [Password]: 1234admin [Status]: Failed
[Attempt]: 11 [Username]: admin [Password]: 1502 [Status]: Failed
[Attempt]: 12 [Username]: admin [Password]: 166816 [Status]: Failed
[Attempt]: 13 [Username]: admin [Password]: 21241036 [Status]: Failed
[Attempt]: 14 [Username]: admin [Password]: 2222 [Status]: Failed
[Attempt]: 15 [Username]: admin [Password]: 22222 [Status]: Failed
[Attempt]: 16 [Username]: admin [Password]: 240653C9467E45 [Status]: Failed
[Attempt]: 17 [Username]: admin [Password]: 266344 [Status]: Failed
[Attempt]: 18 [Username]: admin [Password]: 3477 [Status]: Failed
[Attempt]: 19 [Username]: admin [Password]: 3ascotel [Status]: Failed
[Attempt]: 20 [Username]: admin [Password]: 3ep5w2u [Status]: Failed
[Attempt]: 21 [Username]: admin [Password]: 3ware [Status]: Failed
[Attempt]: 22 [Username]: admin [Password]: 4getme2 [Status]: Failed
[Attempt]: 23 [Username]: admin [Password]: 4tas [Status]: Failed
```

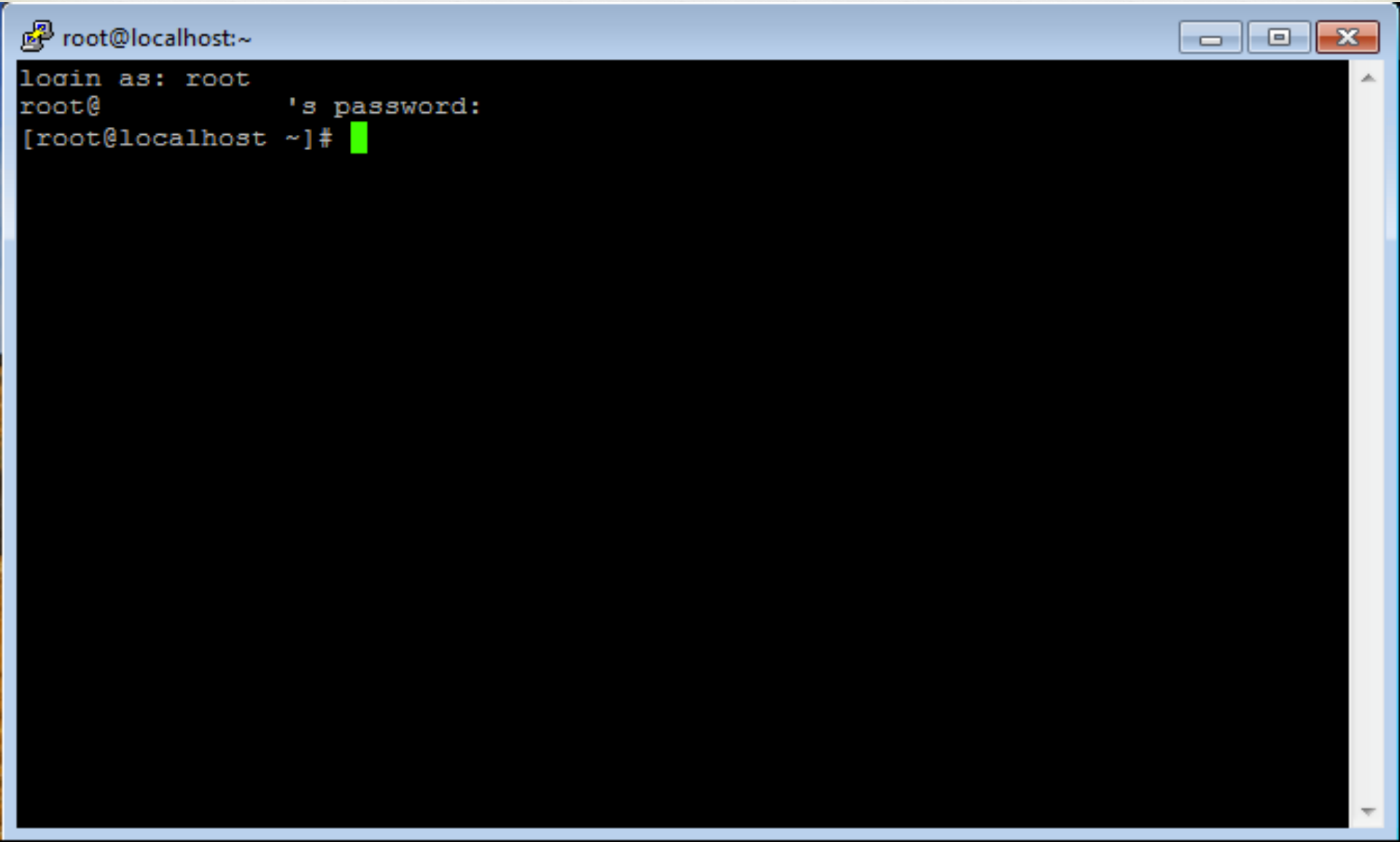
Gaining Access to the Target Computers



Warning


client@localhost:~
login as: client
client@[redacted]'s password:
The actual or attempted unauthorized access, use,
or modification of this system is strictly prohibited.
Unauthorized users are subject to Institutional disciplinary
proceedings and/or criminal and civil penalties under state,
federal, or other applicable domestic and foreign laws.
The use of this system is monitored and recorded for
administrative and security reasons.
Anyone accessing this system expressly consents to such monitoring
and is advised that if monitoring reveals possible evidence of
criminal activity, the Institution may provide the evidence of
such activity to law enforcement officials.
[client@localhost ~]$

No Warning


root@localhost:~
login as: root
root@ 's password:
[root@localhost ~]#

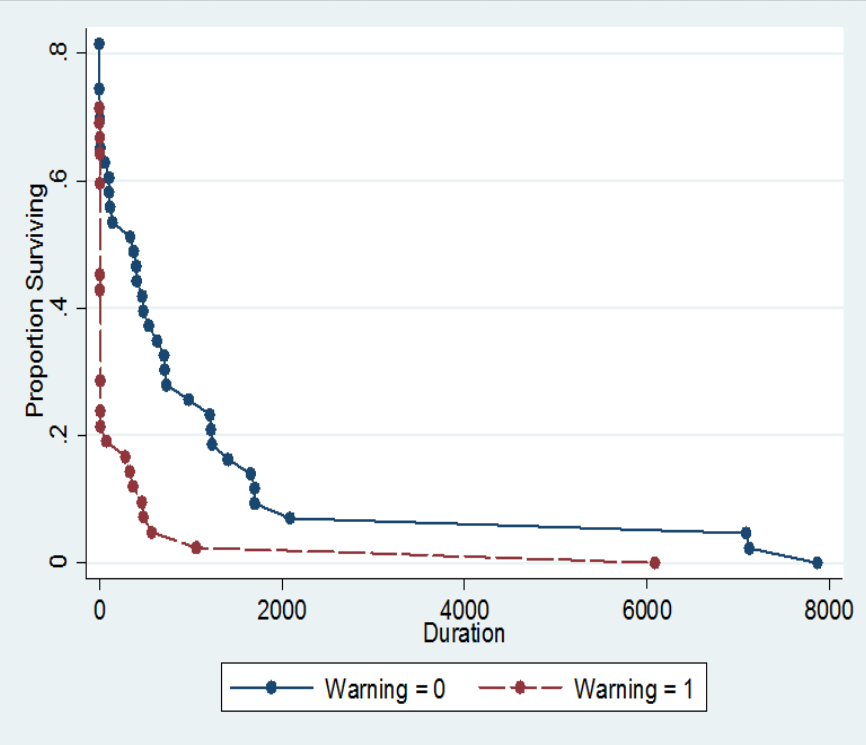
Immediate Termination of System Trespassing Event

Frequency of Repeated System Trespassing Events

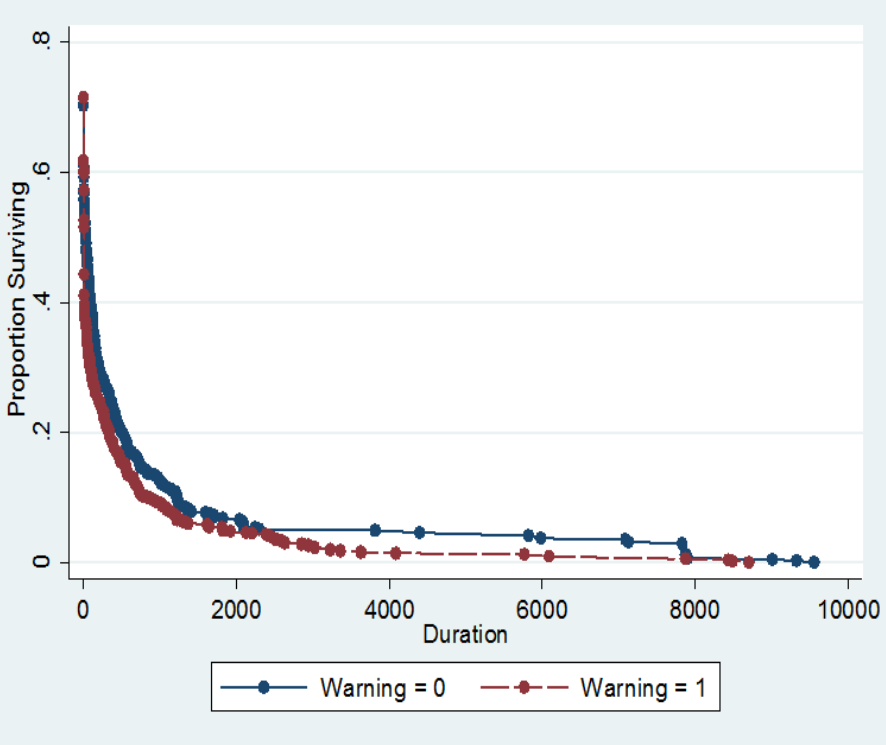
Time to System Trespassing Incident Termination

Time to System Trespassing Incident Termination

First Incidents (N =86)



All Incidents (N= 971)



Experiment #1a : Design

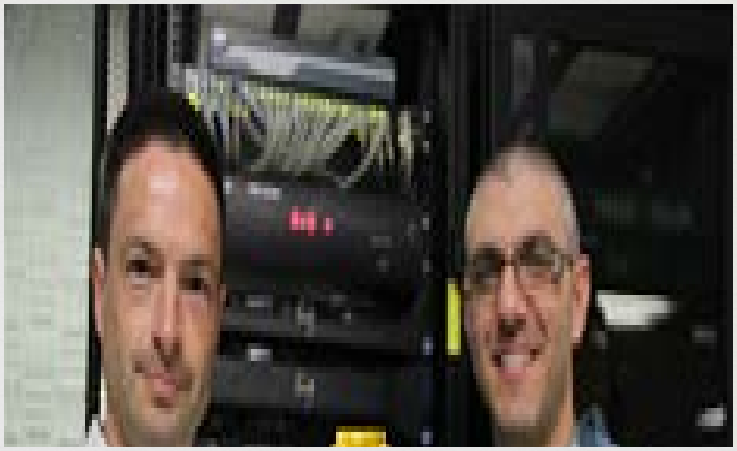
- 300 IP addresses
- Experimental period: 6 months
- Waited…..
- Simulated a genuine environment
- Systematic assignment/allocation

Type	Memory	Disk Space	Bandwidth	Banner
	0=2.25GB	0=30GB	0=512Kbit/s	0=No Banner
	1=512MB	1=5GB	1=128Kbit/s	1=Banner

Immediate Termination of System Trespassing Event

Frequency of Repeated System Trespassing Events

Time to System Trespassing Incident Termination



Humans are ambiguity averse

Humans are ambiguity averse

The presentation of ambiguous information regarding the presence of surveillance will INCREASE system trespassers' active efforts to avoid detection

The presentation of ambiguous information regarding the presence of surveillance will REDUCE system trespassers' active efforts to avoid detection

Experiment #2 : Design

- 300 IP addresses
- Experimental period: 6 months
- Waited…..
- Simulated a genuine environment

No Surveillance

Control

root@localhost:~

```
login as: root
root@           's password:
[root@localhost ~]#
```

Surveillance Software

Treatment 1 (high ambiguity)


```
 3419 ?        Sl     0:00 /sbin/rsyslogd -c 4
 3431 ?        Ss     0:00 /usr/sbin/sshd
 3438 ?        Ss     0:00 xinetd -stayalive -pidfile /var/run/xinetd.pid
 3448 ?        Ss     0:00 /usr/sbin/saslauthd -m /var/run/saslauthd -a pam -n 2
 3453 ?        S      0:00 /usr/sbin/saslauthd -m /var/run/saslauthd -a pam -n 2
 3468 ?        Ss     0:20 sendmail: accepting connections
 3475 ?        Ss     0:00 sendmail: Queue runner@01:00:00 for /var/spool/client
 3483 ?        Ss     0:02 /usr/sbin/httpd
 3485 ?        S      0:00 /usr/sbin/httpd
 3491 ?        Ss     0:01 crond
 5425 ?        S      0:00 /usr/sbin/httpd
23568 ?        S      0:03 /usr/bin/perl /bin/monitor
23588 ?        SN     0:00 /usr/sbin/zabbix_agentd
23596 ?        SN     0:08 /usr/sbin/zabbix_agentd
23598 ?        SN     0:00 /usr/sbin/zabbix_agentd
23599 ?        SN     0:00 /usr/sbin/zabbix_agentd
23600 ?        SN     0:00 /usr/sbin/zabbix_agentd
23601 ?        SN     0:00 /usr/sbin/zabbix_agentd
28309 ?        Ss     0:00 sshd: test [priv]
28323 ?        S      0:00 sshd: test@pts/0
```

Surveillance Banner

Treatment 2 (medium ambiguity)


```
test@                's password:

This system is under continuous surveillance. All user activity is being monitor
ed and recorded.

[test@localhost ~]$
```

Surveillance Banner and Software

Treatment 3 (low ambiguity)


```
test@          's password:

This system is under continuous surveillance. All user activity is being monitor
ed and recorded.

[test@localhost ~]$
```

```
3419 ?        Sl     0:00 /sbin/rsyslogd -c 4
3431 ?        Ss     0:00 /usr/sbin/sshd
3438 ?        Ss     0:00 xinetd -stayalive -pidfile /var/run/xinetd.pid
3448 ?        Ss     0:00 /usr/sbin/saslauthd -m /var/run/saslauthd -a pam -n 2
3453 ?        S      0:00 /usr/sbin/saslauthd -m /var/run/saslauthd -a pam -n 2
3468 ?        Ss     0:20 sendmail: accepting connections
3475 ?        Ss     0:00 sendmail: Queue runner@01:00:00 for /var/spool/client
3483 ?        Ss     0:02 /usr/sbin/httpd
3485 ?        S      0:00 /usr/sbin/httpd
3491 ?        Ss     0:01 crond
5425 ?        S      0:00 /usr/sbin/httpd
23568 ?       S      0:03 /usr/bin/perl /bin/monitor
23588 ?       SN     0:00 /usr/sbin/zabbix_agentd
23596 ?       SN     0:08 /usr/sbin/zabbix_agentd
23598 ?       SN     0:00 /usr/sbin/zabbix_agentd
23599 ?       SN     0:00 /usr/sbin/zabbix_agentd
23600 ?       SN     0:00 /usr/sbin/zabbix_agentd
23601 ?       SN     0:00 /usr/sbin/zabbix_agentd
28309 ?       Ss     0:00 sshd: test [priv]
28323 ?       S      0:00 sshd: test@pts/0
```

Clean Tracks Commands

- Remove a file (rm-rf)
- Delete history (unset)
- Clear bash history (history)
- At least one clean tracks command

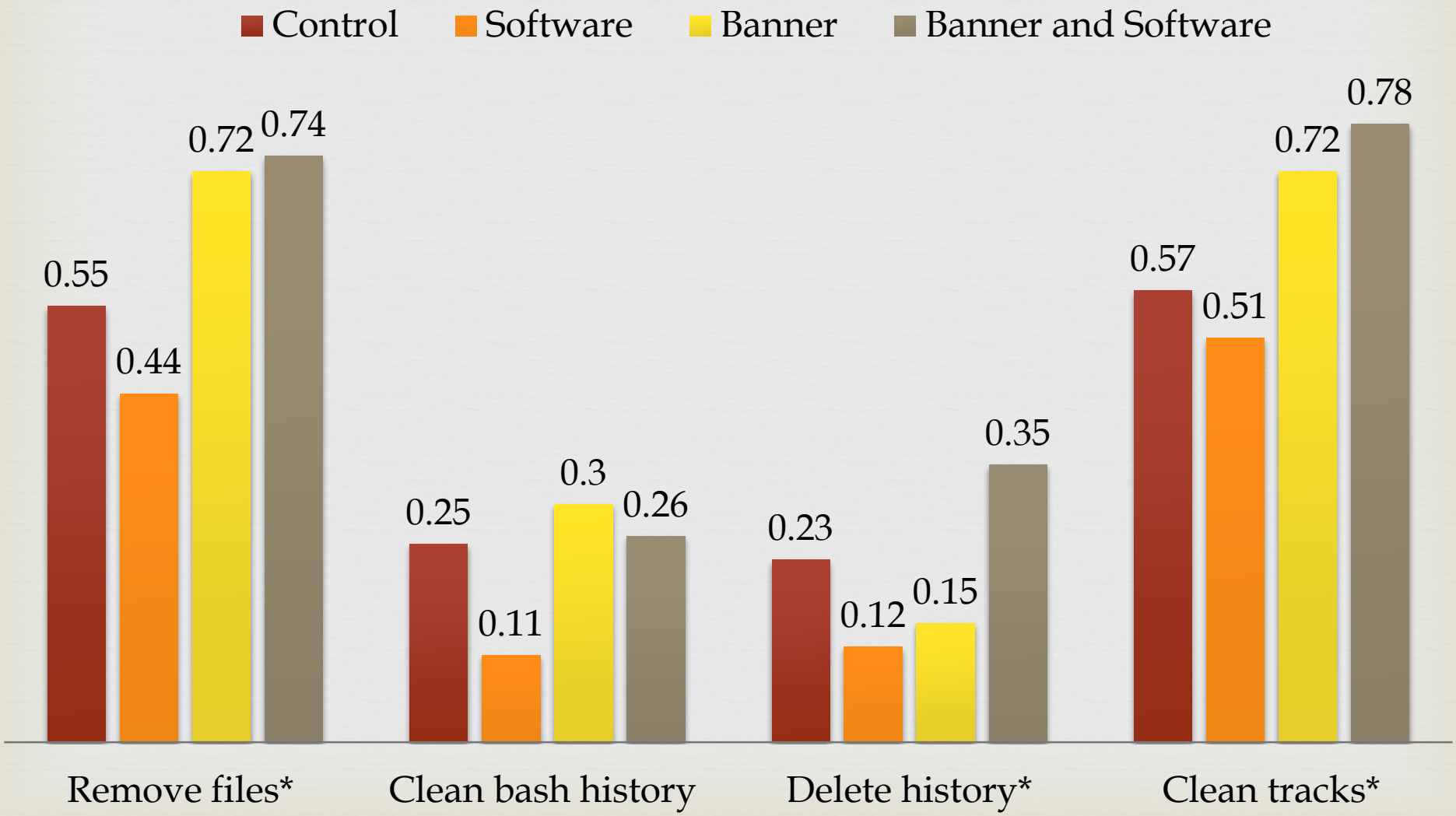
Two Groups

N = 268 Systems

N =190 Systems

No significant differences were found between the proportions of surveillance banner and no surveillance banner target computers with clean track commands

Proportions of Target Computers Presenting Different Levels of Ambiguity Regarding the Presence of Surveillance with Clean Track Commands (N=190 Target Computers)



Cleaning Tracks Commands are 2.67 times more likely to be Found on Attacked Computers with Surveillance Banners and Software Installed on

VS.

Surveillance in Non-Cyber Environments

Natural Surveillance

Surveillance by Place Managers

Surveillance in Cyber Environments

Natural Surveillance

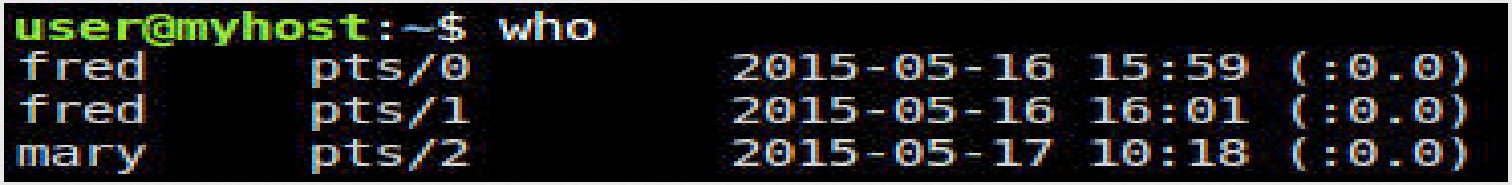
Surveillance by Place Managers

Experiment #4 : Design

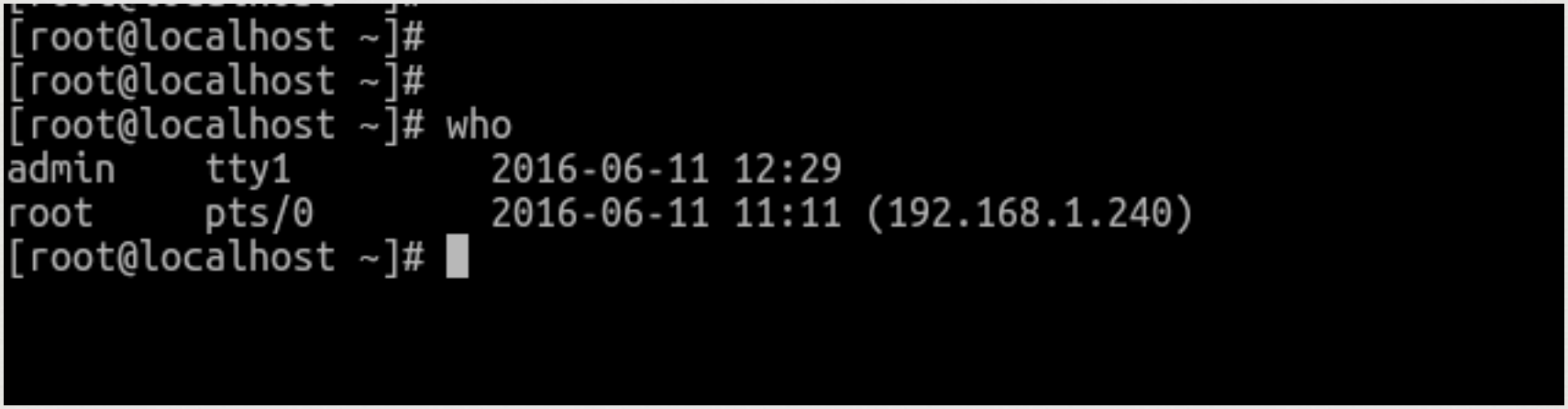
- 300 IP addresses
- Experimental period: 6 months
- Waited…..
- Simulated a genuine environment

Control: No Users Logged

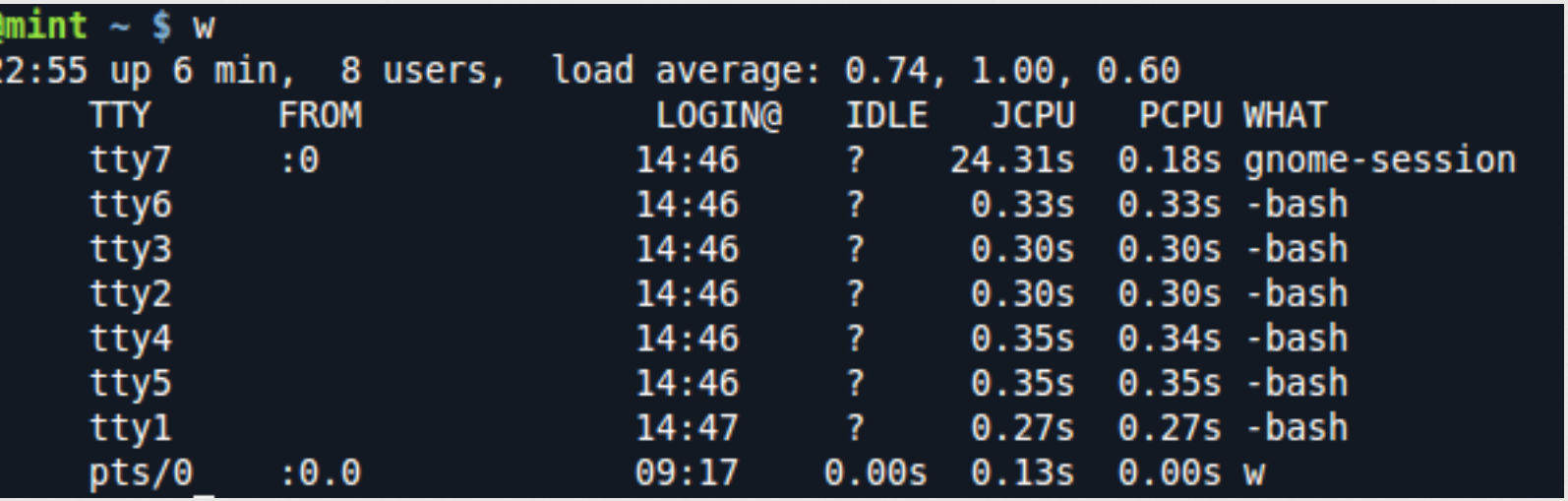
Treatment 1: Non-Admin User



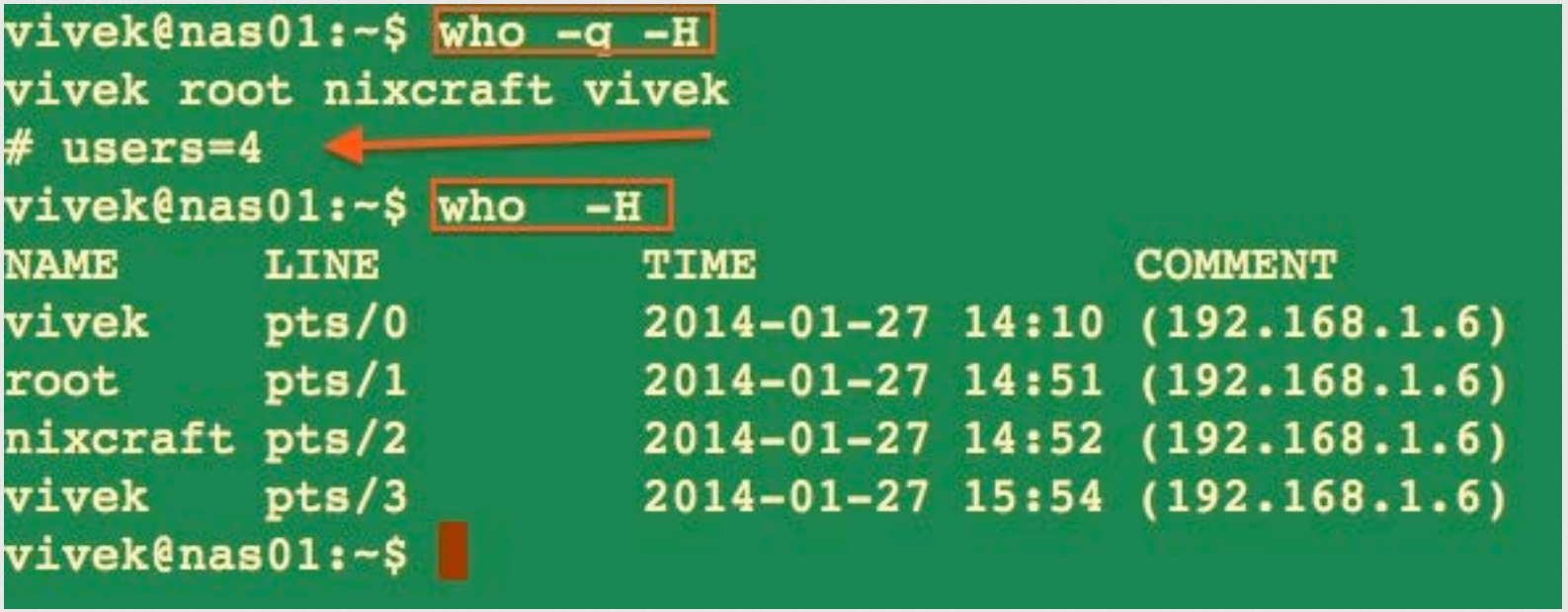
Treatment 2: Admin User



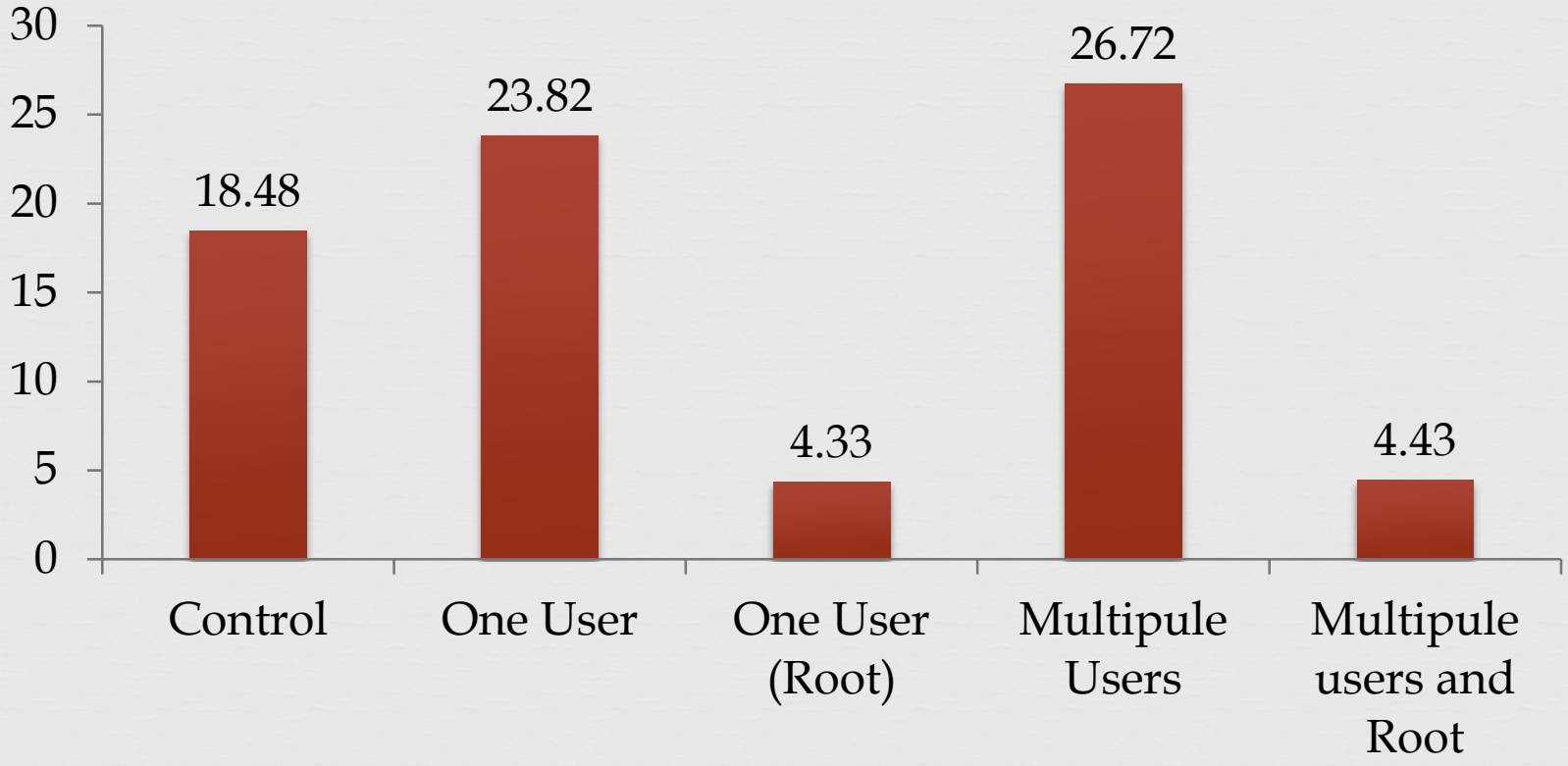
Treatment 3: Ten Non-Admin User



Treatment 4: Nine Non-Admin and One Admin User



Mean Number of System Trespassing Events (N=251 Computers)



What Do Our Findings Suggest?

Can These Findings Support the Resilience of Fortress Computing Environments?

In Conclusion,

- Evidence regarding human behaviors on computer environments is relevant for improving computer users' and IT professionals' ability to detect, report and respond to security issues.

- Future applications of "soft sciences" models are crucial for generating more sophisticated security solutions for both bazaar and fortress computing environments

David Maimon
Email: dmaimon@umd.edu
Website: www.davidmaimon.net
Twitter: @david_maimon