METRO-GOLDWYN-MAYER presents

A GEORGE PAL PRODUCTION

H.G. WELLS' THE TIME MACHINE

in futuristic METROCOLOR

YOU WILL ORBIT INTO THE FANTASTIC FUTURE!

STARRING

ROD TAYLOR

ALAN YOUNG · YVETTE MIMIEUX

SEBASTIAN CABOT · TOM HELMORE

Screen Play by DAVID DUNCAN · Based on the Novel by H. G. WELLS · Directed by GEORGE PAL

Who am I, what is this…

- I'm Steve Romig: romig@acm.org, @romig on twitter
- This is about a security investigation from the mid-90s, some tools we made, some things we learned. I might also make some useful observations.
- I'm not trying to poke fun at the intruders, or at least, not any much more than I am at myself…

Pre-incident (1995/1996)

- OSU didn't have much of an incident response team: inconsistent, ad-hoc process; useless paper records.
- They had recently hired me to “do security” part-time
  - I started tracking incidents, logging auth and network activity.
  - We started education/awareness meetings (SECWOG)

Awareness meetings really facilitated formation of a formal incident response team, by the way – generated lots of good will, spirit of cooperation, etc.

One take-away: be a community organizer!

UPSET HIS COFFEE.

August 27, 1996, 7 PM

- A California ISP calls me at home: they'd been compromised
  - Attack came via our modem pool.
  - They named a suspect: someone using the nickname XXX on IRC.
- I confirmed the activity
  - Intruder had been logged in through modem pool since 2:00 that morning.
  - We had several previous incidents for this intruder
- I was ~~pissed off motivated~~ pissed off and motivated - they interrupted play time

Confirmed activity through network traffic logs, identified account through authentication logs, checked previous incidents involving XXX through our incident tracking system.

I received a phone call @home from an ISP in California while I was playing with my kids. The ISP claimed that they had been compromised from an OSU IP address. Earlier in the day they had been in an IRC (Internet Relay Chat) conversation with someone using the nickname XXX who had asked for a shell account in exchange for telling them about their security problems. They were actually considering this when the break in occurred.

I confirmed the attacks through our network traffic logs. Some quick work with our authentication logs for the modem pool revealed that the account used to authenticate belonged to a student in our medical school - an unlikely cracker. A quick look through our incident logs revealed that we had had several (5?) previous incidents involving someone using the nickname XXX on IRC, all coming through our modem pool, and using several different accounts.

Tentative conclusion: someone (not the med student) had a way to steal accounts, and was using them to gain free access to the internet through our modem pool, where they'd wreak mischief.

Some lessons to be learned: publish your contact info; log lots, log often, retain your logs; early action can prevent later nastiness.

August 28, 12:30 AM

- Long story short: I try to trace a phone call in the middle of the night, almost talk a bunch of bored phone switch engineers into tracing the call without a court order, learned more about phone systems than I ever wanted to know, discovered that we couldn't get the trace done this way, but in the end learned how to do it the right way. When we tried to do it the right way the company and the court disagreed about the correct legal vehicle to get the work done.
- The intruder hung up after 36 hours on the phone.

Capture all the packets…

August 29, 1996

- We set up tcpdump logging of intruder sessions.
- We had to identify sessions through our authentication logs and start/stop tcpdump by hand.
- This raised legal concerns: what about the ECPA? We talked to our lawyer – they said "no"

The ECPA (Electronic Communications Privacy Act) is a tough law to interpret, and there's little case law to help.

Our lawyer determined, after consulting with the U.S. Department of Justice, that our actions were OK.

Talk to your lawyers.

Create an incident response "team", not necessarily full time: right players, know each other.

Key players: legal, IT, communications, student affairs, help desk, etc.

Make a plan – who decides how/whether incidents will be handled.

Test your plan!

September 3, 1996

» We got tired of starting tcpdump by hand
» So we bought a copy of Phantom wrote tacacs-action
  – A config file lists accounts to watch and the actions to take on login/logout for those accounts.
  – Actions include "log" and "page"
  – "page" does what you'd expect
  – "log" invokes tcpdump on a sniffer on the correct subnet to capture their traffic on login (filtering for just their IP address), or stops tcpdump for that session on logout.

Was amused with hacker-on, hacker-off pages. They'd come home from school - login, login, login. Break for dinner - logout, logout, logout. After dinner - login, login, login. They decide to see a movie - logout, logout, logout. Playing quake at home after movie - login, login, login.

September 5, 1996

- I got insanely tired of getting paged all the time, so I turned off the paging action in the tacacs-action control file.
- We discovered that several people were using compromised accounts and some were using the same account.
- We discovered that one of the local groups hangs out in #614 on IRC, so I started lurking in #614

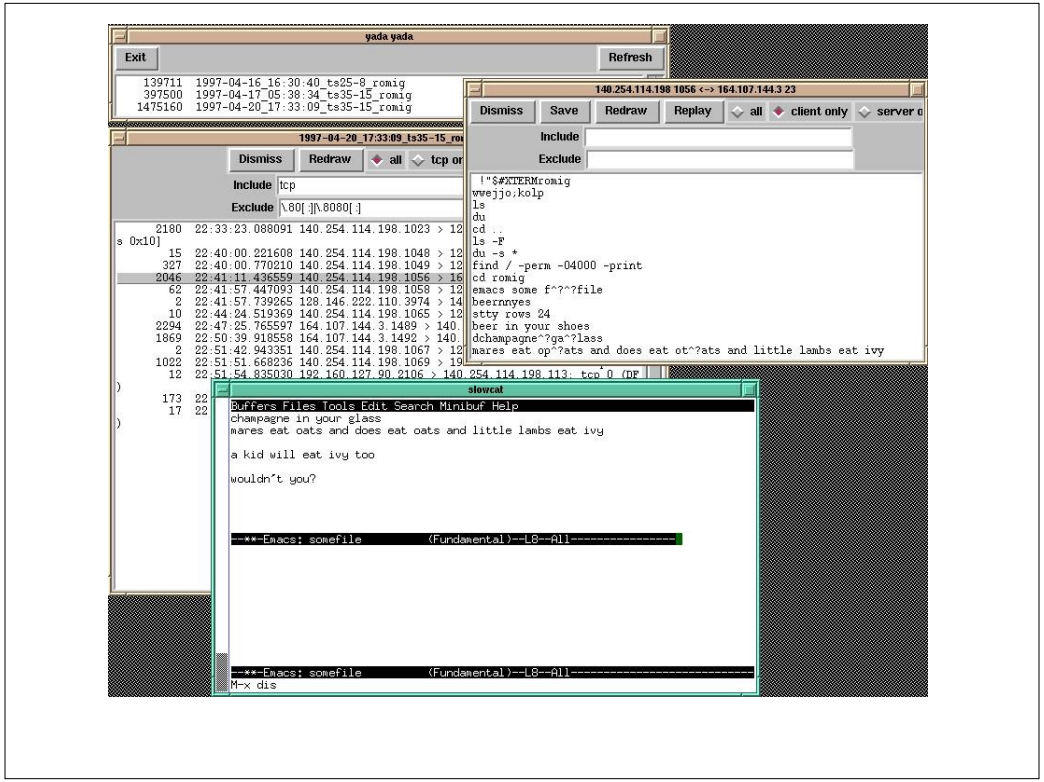
Meanwhile…

- The Tcpdump logs are piling up
- We read through the logs with tcpdump and strings (yes, believe it or not) and a program called cleanup that Mark Fullmer wrote.
- This is tedious, icky, and prone to errors. It is hard to read terminal escape sequences and other “obfuscated” traffic.

Automation!

I wrote “Review”

» Review is a Perl script with a Tk GUI that makes it easier to browse a list of “pcap” files, see a summary of the sessions in each, and look at the content of those sessions in several different ways.



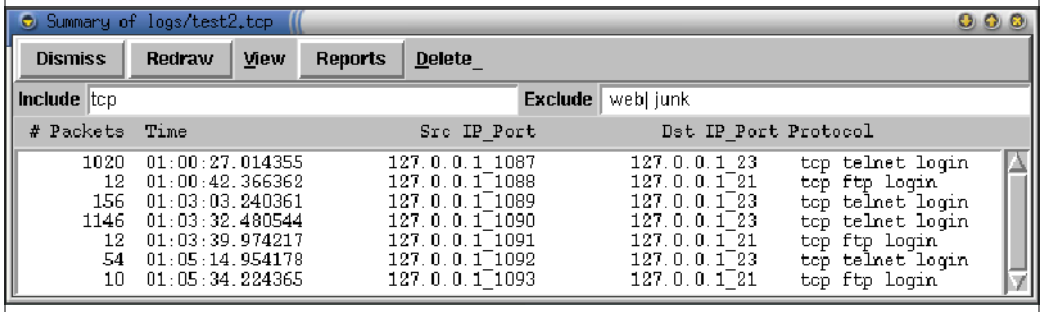
This is a set of the typical windows that you might see when using review – top left is the “log listing” window, middle left is the “session summary” window that shows what sessions are within a selected log file, upper right is a “session content” window, and bottom middle is a replay of a telnet/rlogin session showing what should have appeared on the target’s screen.

Log Listing Window

» List of logs, sizes
» Double click log to see summary

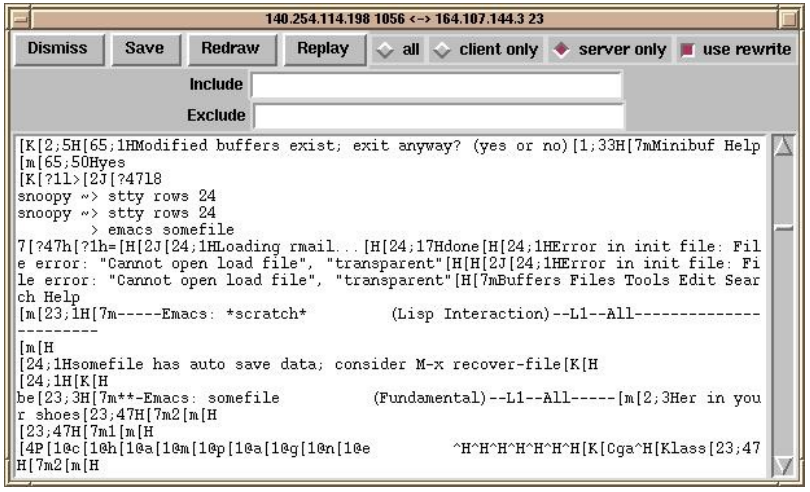
Session Summary Window

- Shows sessions from one log
- Double click to see contents
- Filter (include/exclude) by string match, including “tags”



We like numbers – IP addresses and TCP/UDP port numbers. Names are useful, but can be misleading. Various tricks can cause your system to report incorrect names for IP addresses (DNS cache poisoning, domain takeovers, etc.) And people can set up any service to run on any port number. Just because TCP/80 is usually a web server doesn’t mean that its always a web server.

Session Contents

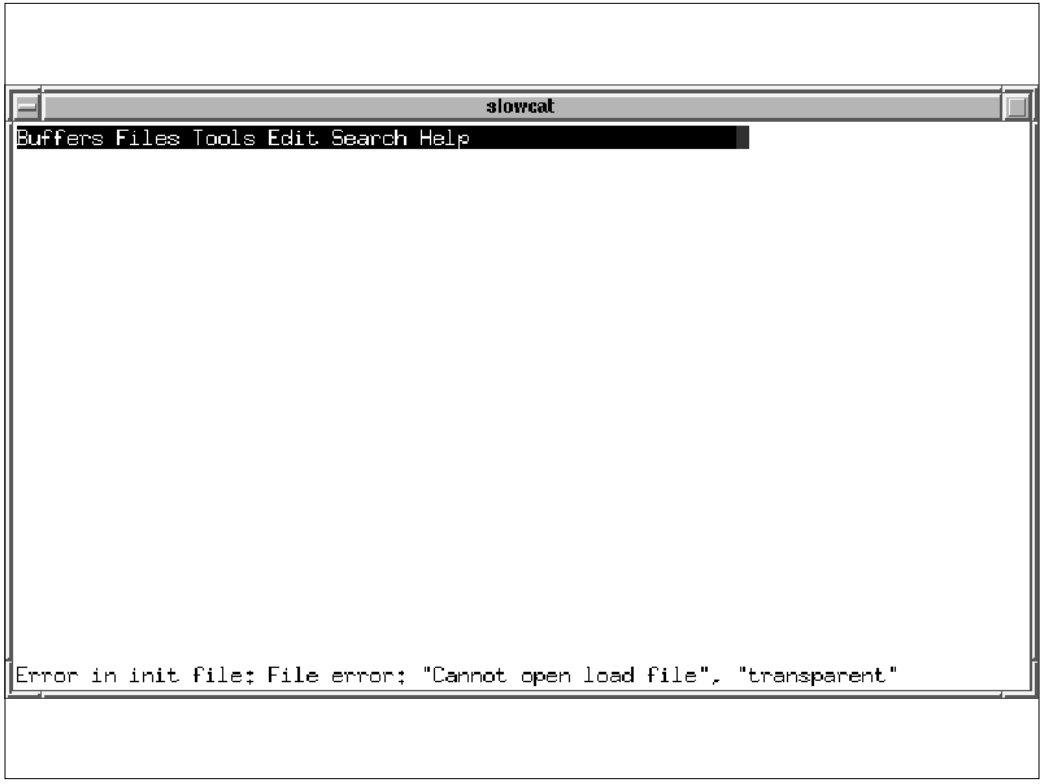


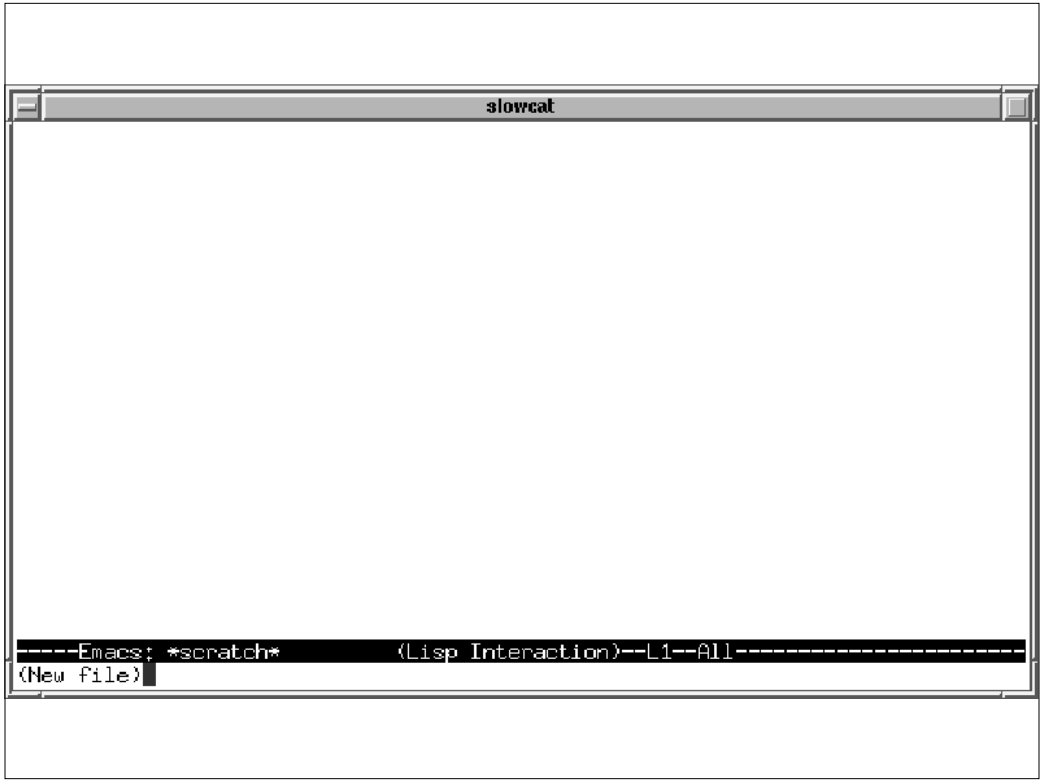
This shows the printable characters from the server->client traffic for a telnet session. In this case, the target was using “emacs”, which uses terminal escape-sequences to manipulate the appearance of the screen/terminal emulator. This makes it hard to see what the suspect is doing – pulling out the printable contents isn’t very meaningful.

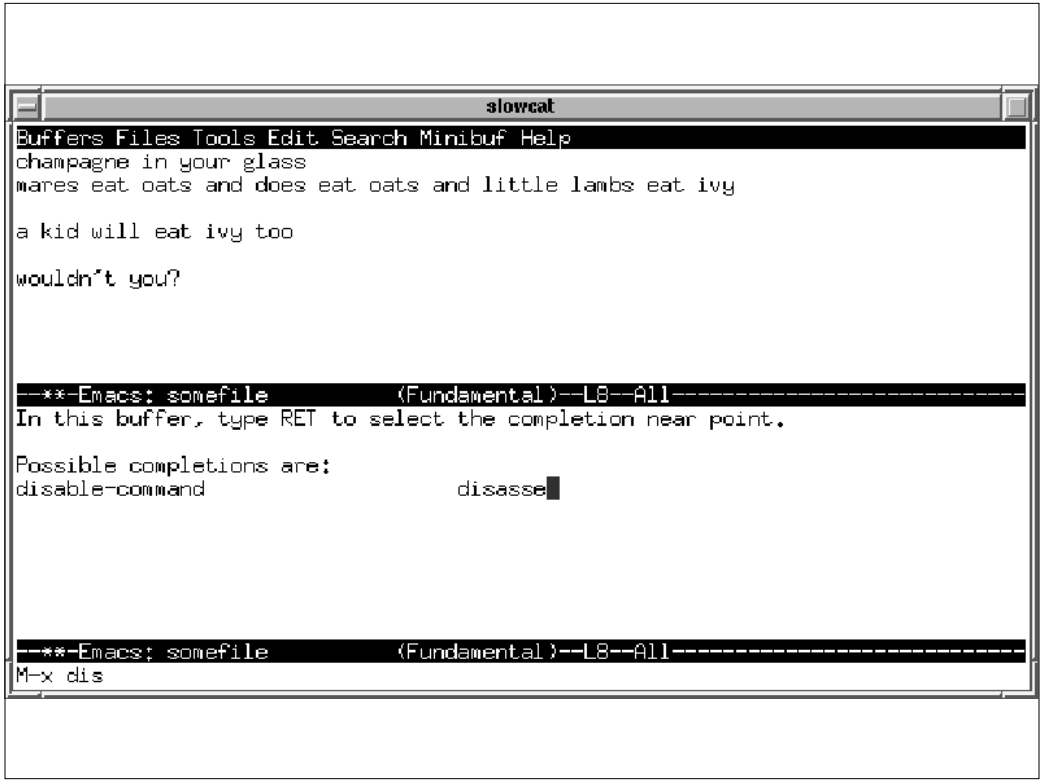
Session Replay

» Escape sequences are hard to read
» Replay takes the server to client traffic and writes it at a controlled rate to a terminal emulator

Here's what it looks like when we "replay" the reconstructed server->client traffic in a terminal emulator at a controlled rate.


slowcat
Buffers Files Tools Edit Search Help
Error in init file: File error: "Cannot open load file", "transparent"


slowcat
-----Emacs: *scratch* (Lisp Interaction)--L1--All----------
(New file)



This is lots easier to read.


EMERGENCY

September 13, 1996

- My morning ritual - check mail, download tcpdump logs, run the pre-processing stuff, get a cup of coffee, and settle down to read.
- They were doing lots of IRC, email, some probing, some exploits.
- They used SSH and PGP
  - Through telnet sessions
  - Sent pass-phrases for private keys via telnet
  - Sent private keys via FTP and IRC

In one conversation in IRC, XXX was discussing the importance of not using plain text sessions (e.g. telnet). "I never login through telnet, I always use ssh." He was logged in through telnet, of course.

They sometimes used ssh and pgp. Fortunately, they usually telnet'd to the box that they'd run ssh and pgp from, so I had copies of *everything* - their password for that account, passphrases for their ssh and pgp private keys, etc. Had copies of several of the private keys because they transferred them with FTP or IRC in plain text.

One guy was fairly savvy - always used ssh, and always encrypted his email. Fortunately, we could read what "our" crackers said to/read from him, since they usually cc'd each other and we could read the email in their telnet sessions after they had decrypted it.

Weakest link!

When you send encrypted email, encrypt it to your public key also :-(

Ah, breaking news…

- YYY notes that XXX gets accounts by sniffing passwords in an OSU public lab and shares them with friends.
  - Yes, the labs were very sniffable (hubs, not switches, not that that would have been much of a barrier).
  - Yes, plain-text password auth to network services was commonplace at OSU at the time.
  - We had previously recommended fixing both problems, but had been ignored.
- Fix known security problems! Learn from past mistakes!

October 15, 1996

» The first of the military/government intrusions.
» We call the FBI and the various military CERTs.

Phf Exploits

- They were using the canonical "execute xterm on the remote box as root with DISPLAY set to my X server" version of the phf exploit.
- There's some irony to this: for this to work, your X server needs to allow access for the X client on your target.
- My co-worker Tom made a nasty xterm which we ran on a web honeypot, I don't think we ever caught anyone with it though…

Improvements to “Review”

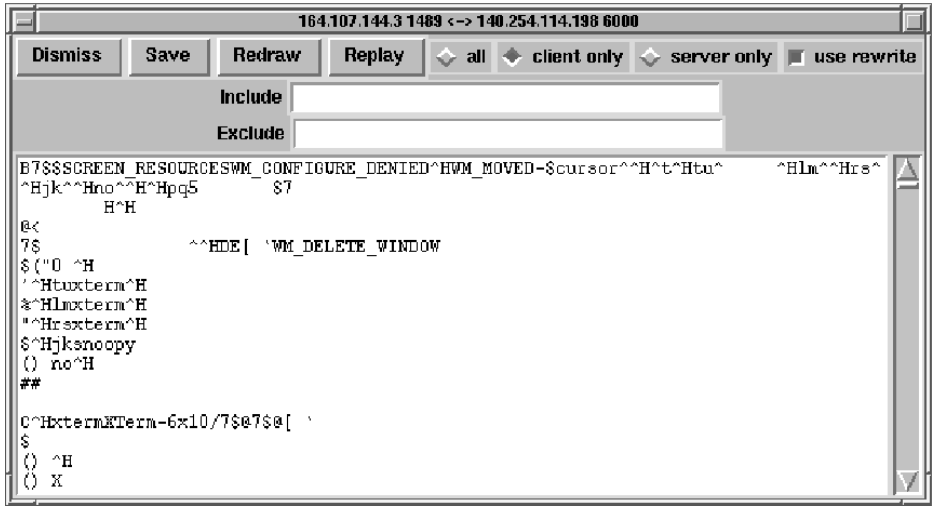
X is Hard

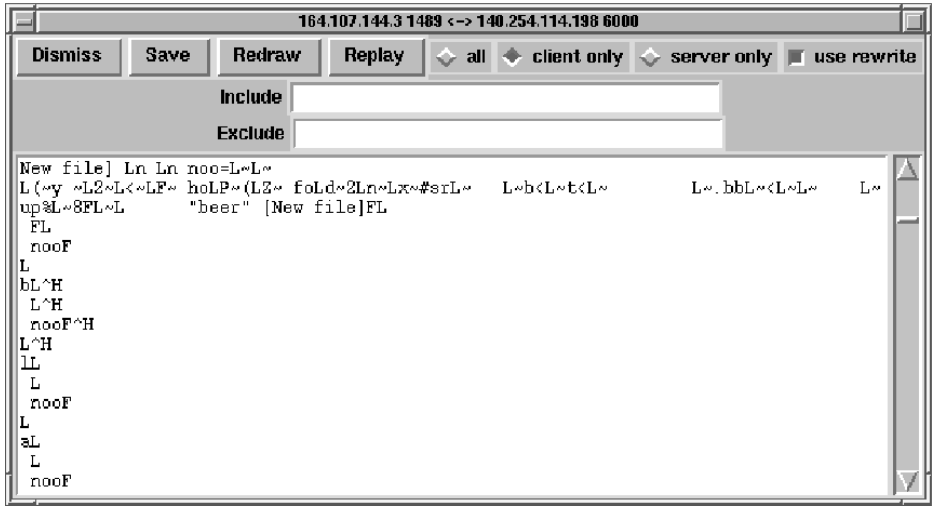
- » X traffic is obscure – requests, results, events are sent in binary form. Server->Client traffic consists of keystroke and mouse events, C->S activity is mostly drawing stuff.
- » I mangled an X debugger called “xmond” to replay X sessions from the tcpdump logs - it reads the C->S packets and passes the safe requests to your X server.
- » Later, Justin Dolske rewrote this in Perl.

Hard to deal with missing packets – resynch problem.

Browsing an X session

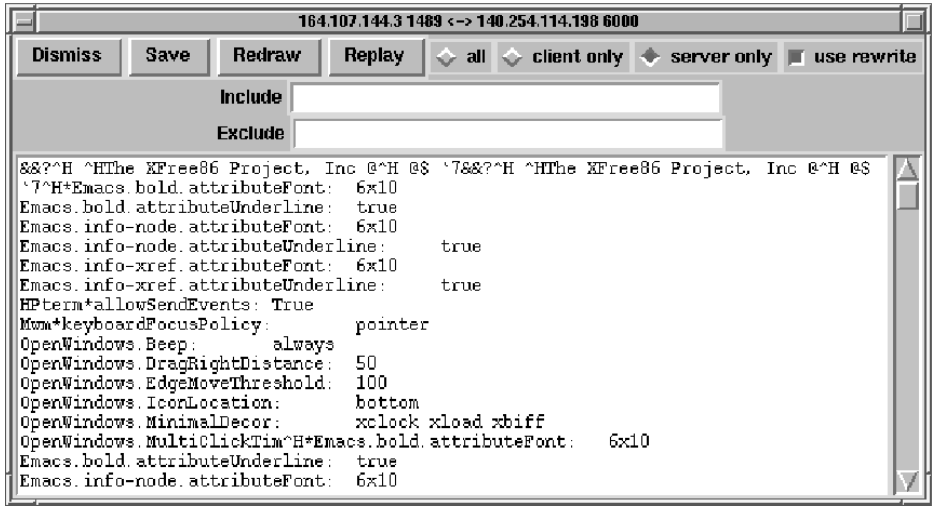
- This is Client->Server traffic (next 2 slides)
- This is what's being drawn on the X server screen for an application (xterm in this case)

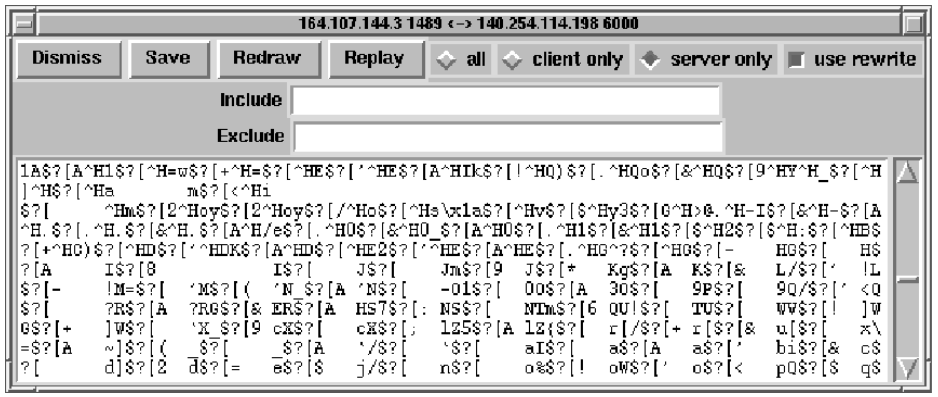

164.107.144.3 1489 <-> 140.254.114.198 6000
Dismiss
Save
Redraw
Replay
all
client only
server only
use rewrite
Include
Exclude
B7$$SCREEN_RESOURCESWM_CONFIGURE_DENIED^HWM_MOVED-$cursor^^H^t^Htu^ ^Hlm^^Hrs^
^Hjk^^Hno^^H^Hpq5 $7
H^H
@<
7$ ^^HDE[`WM_DELETE_WINDOW
$("0 ^H
'^Htuxterm^H
%^Hlmxterm^H
"^Hrsxterm^H
$^Hjksnoopy
() no^H
##
C^HxtermXTerm-6x10/7$@7$@[`
$
() ^H
() X


164.107.144.3 1489 <-> 140.254.114.198 6000
Dismiss
Save
Redraw
Replay
all
client only
server only
use rewrite
Include
Exclude
New file] Ln Ln noo=L~L~
L(~y ~L2~L<~LF~ hoLP~(LZ~ foLd~2Ln~Lx~#srL~ L~b<L~t<L~ L~.bbL~<L~L~ L~
up%L~8FL~L "beer" [New file]FL
FL
nooF
L
bL^H
L^H
nooF^H
L^H
lL
L
nooF
L
aL
L
nooF

Browsing an X session

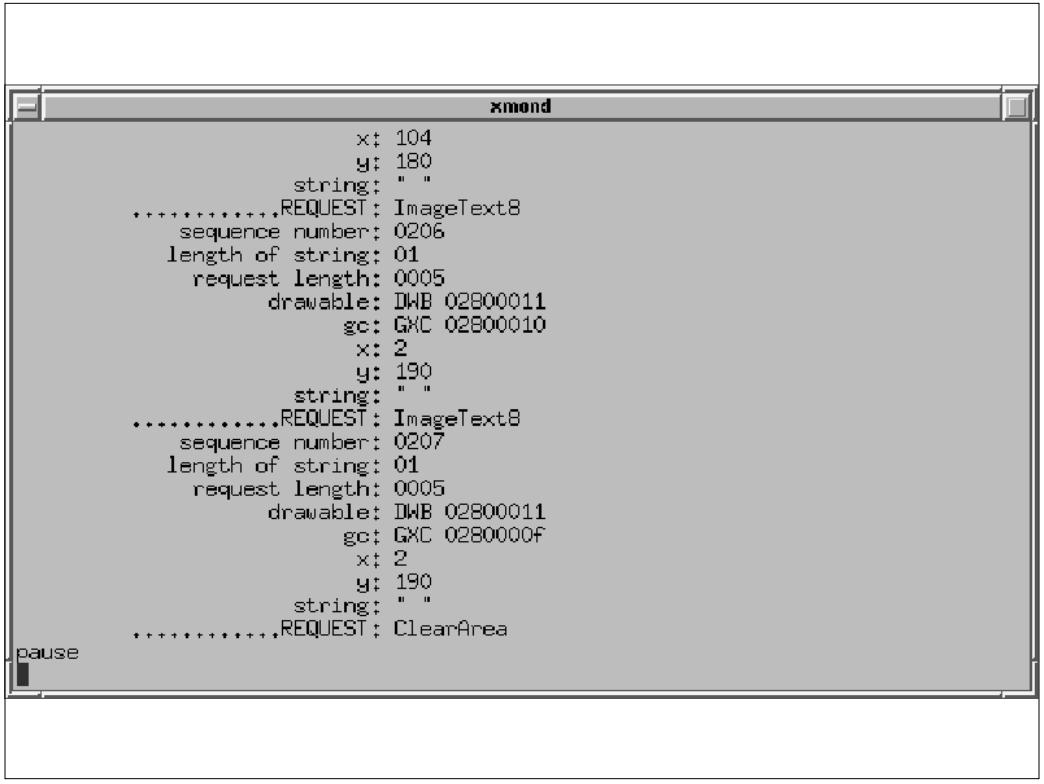
- This is the Server->Client traffic (next 2 slides)
- Mostly keystroke and mouse events sent to this client
- What is the user typing? How would you make sense of the mouse activity?


164.107.144.3 1489 <-> 140.254.114.198 6000
Dismiss
Save
Redraw
Replay
all
client only
server only
use rewrite
Include
Exclude
&&?^H ^HThe XFree86 Project, Inc @^H @$ `7&&?^H ^HThe XFree86 Project, Inc @^H @$
`7^H*Emacs.bold.attributeFont: 6x10
Emacs.bold.attributeUnderline: true
Emacs.info-node.attributeFont: 6x10
Emacs.info-node.attributeUnderline: true
Emacs.info-xref.attributeFont: 6x10
Emacs.info-xref.attributeUnderline: true
HPterm*allowSendEvents: True
Mwm*keyboardFocusPolicy: pointer
OpenWindows.Beep: always
OpenWindows.DragRightDistance: 50
OpenWindows.EdgeMoveThreshold: 100
OpenWindows.IconLocation: bottom
OpenWindows.MinimalDecor: xclock xload xbiff
OpenWindows.MultiClickTim^H*Emacs.bold.attributeFont: 6x10
Emacs.bold.attributeUnderline: true
Emacs.info-node.attributeFont: 6x10

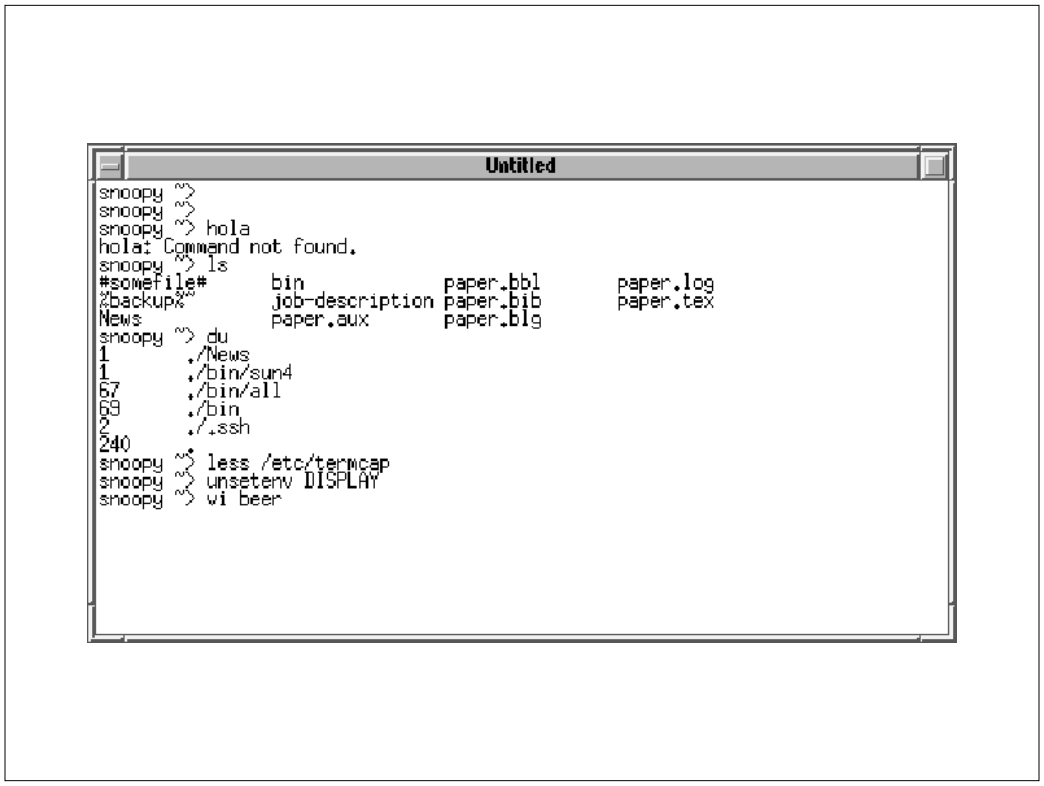

164.107.144.3 1489 <-> 140.254.114.198 6000
Dismiss
Save
Redraw
Replay
all
client only
server only
use rewrite
Include
Exclude

Replay of an X session

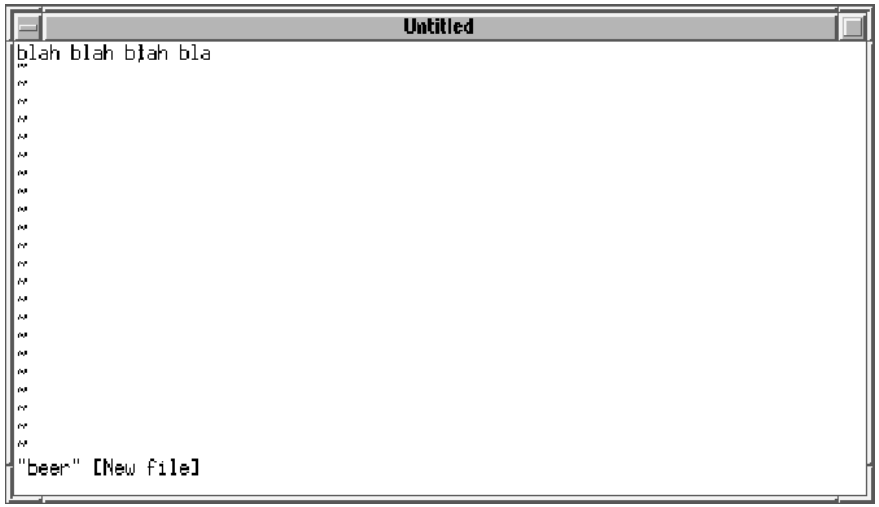
- The next several slides show the results of replaying this session through Review
- The user’s activity is much more obvious now - they were running “vi”
- Works for simple cases, but packet loss can be a huge problem.

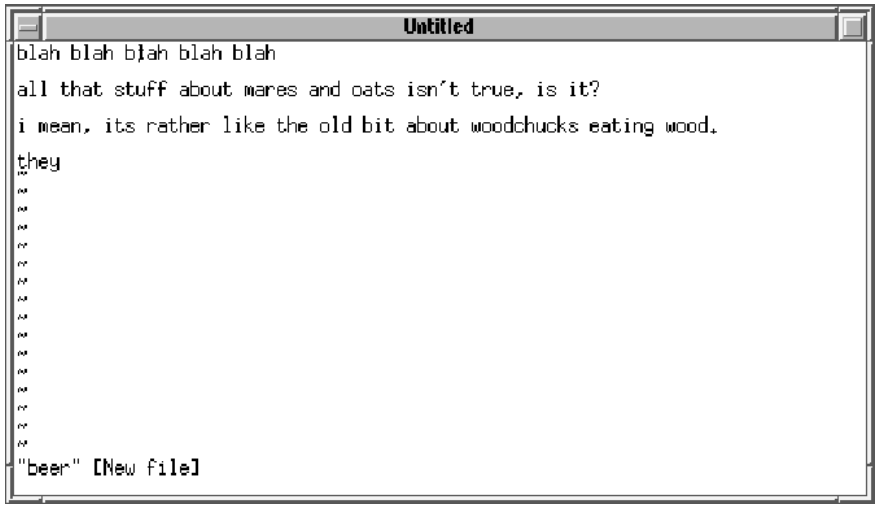


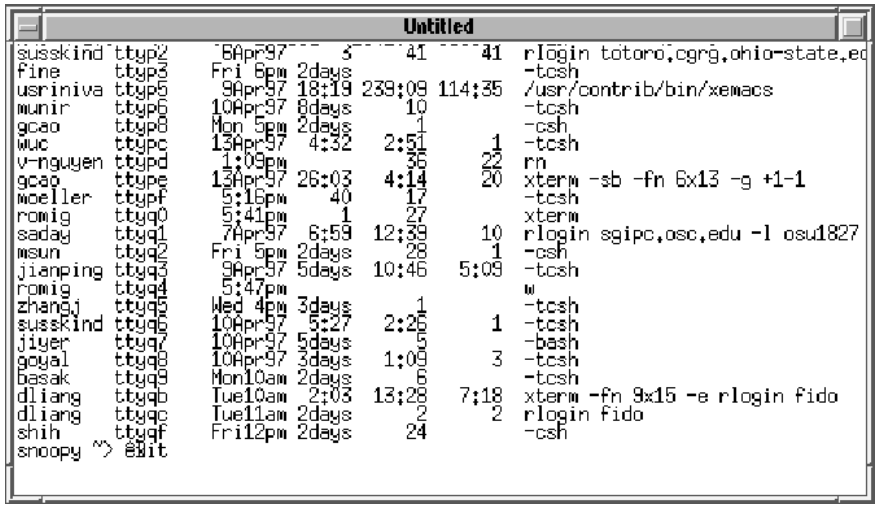
This is output from xmond showing a human-readable interpretation of the requests/responses/events….



This is the reconstructed window for the session: looks like an xterm type application.


Untitled
blah blah blah bla
"beer" [New file]


Untitled
blah blah blah blah blah
all that stuff about mares and oats isn't true, is it?
i mean, its rather like the old bit about woodchucks eating wood.
they
"beer" [New file]


Untitled
susskind ttyp2 8Apr97 5 41 41 rlogin totoro.cgrg.ohio-state.ed
fine ttyp3 Fri 6pm 2days -tcsh
usriniva ttyp5 9Apr97 18:19 239:09 114:35 /usr/contrib/bin/xemacs
munir ttyp6 10Apr97 8days 10 -tcsh
gcao ttyp8 Mon 5pm 2days 1 -csh
wuc ttypc 13Apr97 4:32 2:51 1 -tcsh
v-nguyen ttypd 1:09pm 35 22 rn
gcao ttype 13Apr97 26:03 4:14 20 xterm -sb -fn 6x13 -g +1-1
moeller ttypf 5:16pm 40 17 -tcsh
romig ttyq0 5:41pm 1 27 xterm
saday ttyq1 7Apr97 6:59 12:39 10 rlogin sgipc.osc.edu -l osu1827
msun ttyq2 Fri 5pm 2days 28 1 -csh
jianping ttyq3 9Apr97 5days 10:46 5:09 -tcsh
romig ttyq4 5:47pm w
zhangj ttyq5 Wed 4pm 3days 1 -tcsh
susskind ttyq6 10Apr97 5:27 2:26 1 -tcsh
jiyer ttyq7 10Apr97 5days 5 -bash
goyal ttyq8 10Apr97 3days 1:09 3 -tcsh
basak ttyq9 Mon10am 2days 6 -tcsh
dliang ttyqb Tue10am 2:03 13:28 7:18 xterm -fn 9x15 -e rlogin fido
dliang ttyqc Tue11am 2days 2 2 rlogin fido
shih ttyqf Fri12pm 2days 24 -csh
snoopy ^> exit

I Like Coffee

November 7, 1996

- We learn the real 2600 location – a coffee shop in the 'burbs.
- We started “attending” the meetings (we probably only went to 3 or 4).
- Couldn’t really hear much, but could hear enough to put names to faces and recognize them when they came to the monthly SecWog meetings.
- Max&Erma’s, Rick and his pager…

on one occasion after they moved to the max&ermas at one of the local shopping malls rick and i went and had dinner while they were meeting. i think that was rick's first trip. he thought that one of the kids looked familiar but couldn't place the name or reason. finally he got up to go to the restroom. he returned and we continued talking, but were interrupted by his alpha pager. while he was gone he had found a payphone and called in a description of the kid in question to the osu dispatcher, who paged him with the kid's info - name, address, records, etc. i was amazed...

November-ish, 1996

- We discover that one of the intruders is parking in front of Detective Rick's house every day after school
- A picture's worth a thousand words…

Rick and I were in the habit of trading information about cases we were working on, things like "have you heard of someone who goes by the nick name Blort? Oh, yeah - saw him logging in through the freeness last week." We often found that we could fill in little details for each other on some of the cases we were working on. If nothing else, it helped fill the time while we were waiting for phone tracses to be done.

One night Rick and I were traveling to some meeting, and had a conversation very like the following.

Rick started by asking whether the name "Bob Smith" [not the real name] meant anything to me. Hmmm, nope, couldn't say that it did, though it seemed vaguely familiar. "Why do you ask?" said I.

"Well, I was talking to a couple that live a few doors down from us about their daughter. She's dating a guy who's a self proclaimed computer hacker, says that he likes to break in and see what's there. They said that he works for a local computer company and that he attends Columbus State. I wondered whether that would strike any bells with you."

Well, that was interesting. "Sounds like HipHop", I said jokingly. HipHop is the nickname of one of the hackers we are trying to track down. Unlike most of the rest, we haven't been able to winkle out his name, phone number or home address, although I do know quite a bit about him. He's probably been involved in several dozen major breakins and scores of minor breakins, and the military and FBI have started to take an interest in his activities. We've been trying to trace his calls, with little to show for our efforts so far. That's a whole 'nother story.

"Why, what do you know about HipHop?" asked Rick.

"Well, he's 19 or so, attends Columbus State, works at a local internet service provider. He's the guy that did the military breakins we were talking about last week."

"This fellow is 19, attends CS, works at a computer place."

"Let me guess - her parents hate him?" I asked.

"Yeah! They weren't letting him see her for a month or two. She's in high school..."

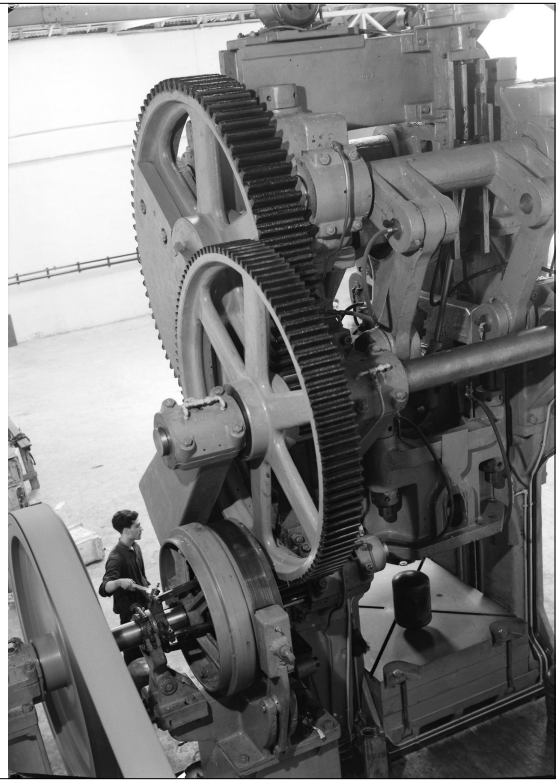
"...Yeah, Worthington? Pretty?"

"Yes!"

February 28, 1997

- The new phone traces are here!
  - 4 boxes of green-bar paper
  - The printout includes obvious email headers - the data was sent from an office in NJ to Columbus, printed and then shipped.
- “We can’t send it electronically”
- “It was never on a computer, sir”
- I had to correlate our list of malicious calls against this, by hand, based on call end time and duration.

Review,
again,
again



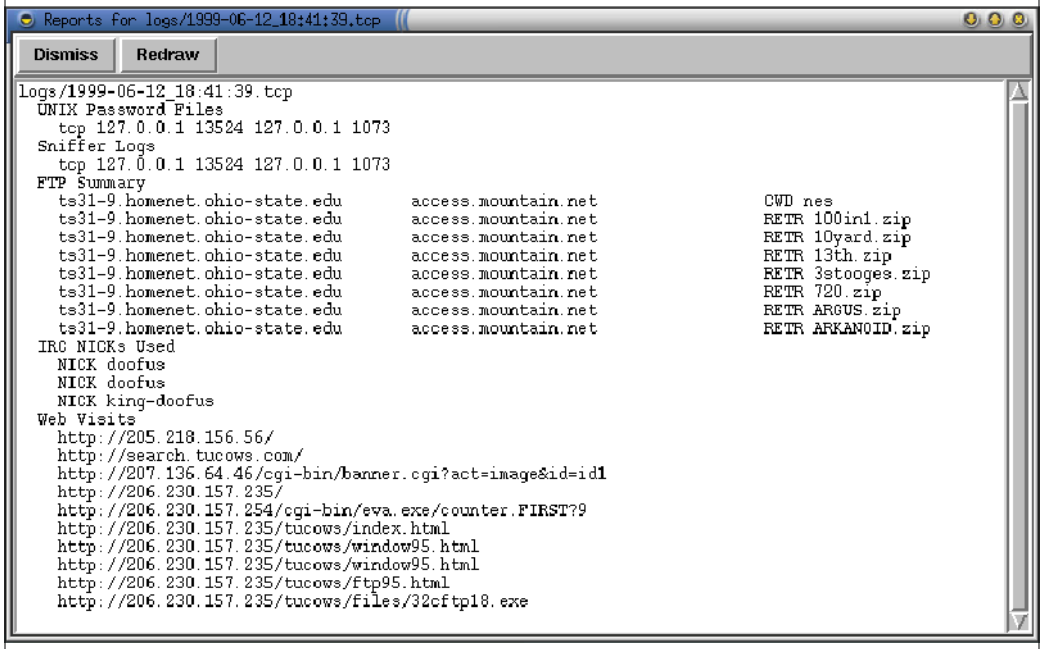
Pete Birkinshaw

Spring, 1997

» A dozen officers from different federal, military investigation groups arrive - FBI, NCIS, OSI
» They have a lot of questions.
» We have documented things well, but the questions go beyond the existing documentation.
» Searching GBs of tcpdump logs for answers is time consuming and tedious.

Report Generator

- So we created a report generator for review.
- For each log file, it lists
  - IRC nicks used
  - Email summary: sender, recipients, subject
  - Files transferred by FTP, IRC DCC SEND
  - URLs visited
  - And it detects some probes, some exploits
- The report is clickable – clicking takes you to the specific TCP session in that log for that element.


Reports for logs/1999-06-12_18:41:39.tcp
Dismiss
Redraw
logs/1999-06-12_18:41:39.tcp
UNIX Password Files
tcp 127.0.0.1 13524 127.0.0.1 1073
Sniffer Logs
tcp 127.0.0.1 13524 127.0.0.1 1073
FTP Summary
ts31-9.homenet.ohio-state.edu access.mountain.net CWD nes
ts31-9.homenet.ohio-state.edu access.mountain.net RETR 100in1.zip
ts31-9.homenet.ohio-state.edu access.mountain.net RETR 10yard.zip
ts31-9.homenet.ohio-state.edu access.mountain.net RETR 13th.zip
ts31-9.homenet.ohio-state.edu access.mountain.net RETR 3stooges.zip
ts31-9.homenet.ohio-state.edu access.mountain.net RETR 720.zip
ts31-9.homenet.ohio-state.edu access.mountain.net RETR ARGUS.zip
ts31-9.homenet.ohio-state.edu access.mountain.net RETR ARKANOID.zip
IRC NICKs Used
NICK doofus
NICK doofus
NICK king-doofus
Web Visits
http://205.218.156.56/
http://search.tucows.com/
http://207.136.64.46/cgi-bin/banner.cgi?act=image&id=id1
http://206.230.157.235/
http://206.230.157.254/cgi-bin/eva.exe/counter.FIRST?9
http://206.230.157.235/tucows/index.html
http://206.230.157.235/tucows/window95.html
http://206.230.157.235/tucows/window95.html
http://206.230.157.235/tucows/ftp95.html
http://206.230.157.235/tucows/files/32cftp18.exe


QUAKE
id

Summer 1997

- Tom and I play far too much quake
  - Tom wrote a kick-ass proxy.
  - We both learned lots about the quake protocol…
- Our intruders also play far too much quake…
  - ¼ of the tcpdump logs is quake traffic…
- Heh. What do you think we did?

The original idea for the proxy was that we would both connect to the proxy and it would present itself to the Quake server as a single player. One of us would be the driver, the other would be sort of riding shotgun, able to look and shoot independently. In Quake you can rotate instantly, aim instantly, and change weapons instantly. This would have really rocked :-)

We never got that working. But Tom did make a kick-ass proxy that would automatically select a target, choose a weapon and aim, taking the ammo velocity and the target's direction and velocity into account. You don't want to shoot someone standing next to you with a rocket, and rockets are slow so you need to lead the target by quite a lot to score a hit.

The proxy was deadly. Tom could walk into a room and pull the fire trigger and basically everyone would die.

In Quake, if you die hard enough you frag into pieces. One piece is your head. You aren't

More than you wanted to know about Quake…

- Client tells server where it is moving, what weapon is firing, in what direction
- Server tells the client where it is, what's happening around it
- Client does its rendering based on what direction its looking, location, surrounding events
- Common map information used by both

And Even More About Quake

- You can record “demos” in quake and replay them
- A demo file is essentially a recording of the server to client traffic, with some timing and camera angles thrown in.

“Honestly Boss, We ARE Working…”

- Quake-replay
  - Reads session traffic from a pcap file
  - Massages it with view direction inferred from direction of motion or shooting
  - Constructs a demo recording that you can play
- Now we can see how well our intruders play ☺

Quake exercise actually illustrates several issues about reconstructing events.

Missing packets in this case aren’t a big deal directly, since that happens all the time.

There are limitations to the fidelity of the playback – we can’t know what direction the client was actually looking. Usually, that would be the direction of motion or firing (which is what we use), but they might be side stepping.

See osu.dem – load this into the “id1” directory for your quake client, and type “playdemo osu.dem” to view it.

The end is in sight…

Summer 1997

- The traces all done
  - Confirmed that the intruders are who we thought they were, sigh
  - Get permission to set up pen registers
- Pen registers
  - Record numbers called, caller-id
  - Left running for a month or so

We finally get permission to set up pen registers. These attach to the phone line going to a suspect's house and record the calling number for all incoming calls (caller-id) and the called number for all outgoing calls. Security on these boxes is/was abysmal.

There's a collection station (strange old laptop with lousy software) that receives this information from the devices.

September, 1997

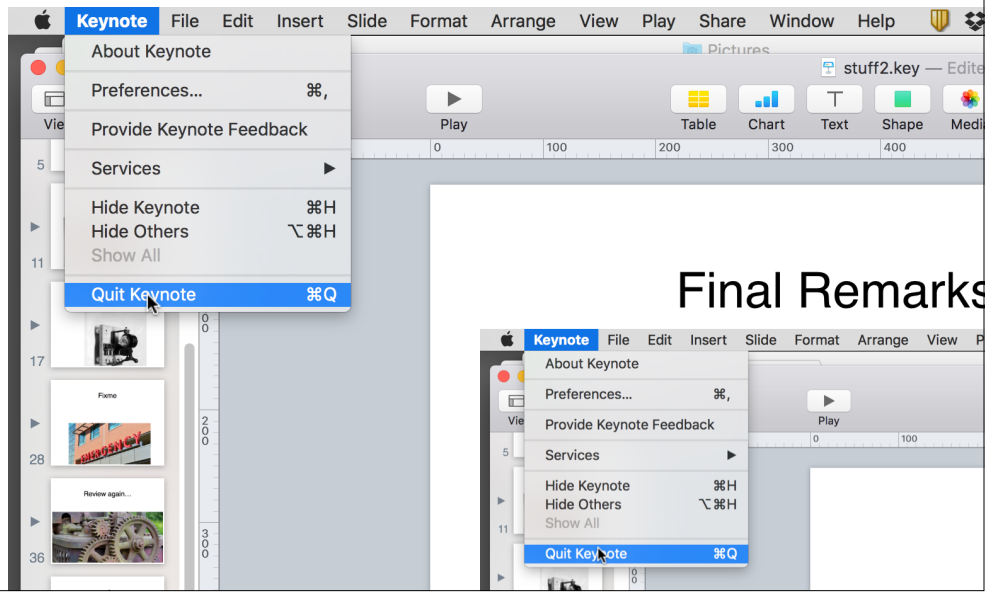
- Search warrants are obtained…
- The night before…XXX says ” i don't worry about breaking in through my accounts at the university because they'll never catch me..."
- They arranged to serve all 9? simultaneously at 7 AM.
- Coffee and donuts with a few dozen officers…

Fini

End result: the Federal Law Enforcement groups spent about 2 years looking at things before deciding not to pursue charges. Turned it over to the State, which also declined to do anything.

We often joked that we should've just walked into the coffee shop, pulled up a chair at their table, thrown down a pile of printouts of their online conversations and said "lets talk"

Final Remarks



Some Observations

- The “black hats” work together better than the white hats do (still)
- Share threat intelligence
- Be a builder (tools, bridges, communities…)
- Hone your incident response process, tools, abilities, etc…
- Hunt!
- Big Data is Bigger, but its always been Big Data
- Stakes have been raised (a lot). We don’t see/worry about teenagers screwing around, we worry about nation-state backed attacks and week-long ddos attacks…