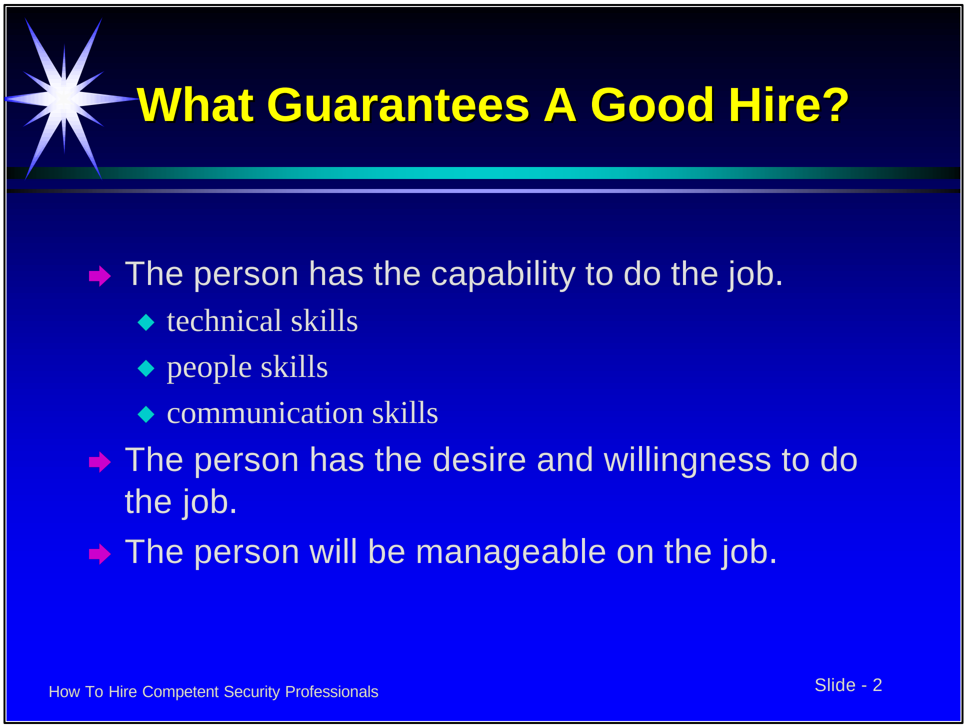
SANS Network Security 99

How To Hire
Competent Security Professionals

Michele D. Crabb-Guel
Cisco Systems, Inc.
mcrabb@cisco.com

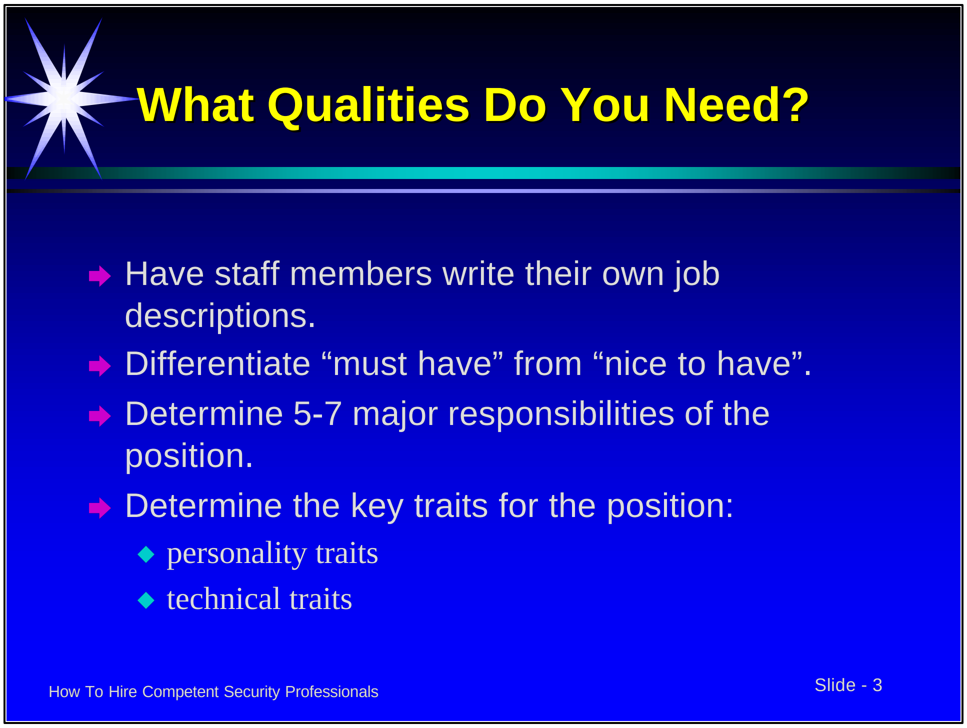
Notes:



What Guarantees A Good Hire?

- The person has the capability to do the job.
  - technical skills
  - people skills
  - communication skills
- The person has the desire and willingness to do the job.
- The person will be manageable on the job.

Notes:



What Qualities Do You Need?

- Have staff members write their own job descriptions.
- Differentiate “must have” from “nice to have”.
- Determine 5-7 major responsibilities of the position.
- Determine the key traits for the position:
  - personality traits
  - technical traits

Notes:

GENERAL DESCRIPTION

Network Security Support will encompass all aspects of UNIX system and network security on multiple architectures (Sun, SGI, HP and IBM workstations, Win/NT Servers).

PRIMARY RESPONSIBILITY

Test, install and maintain security packages/products across multiple platforms.

Provide investigation, coordination, reporting and follow-up of computer network security incidents.

Help define, produce, and maintain official security policy and documentation.

Architect and recommend security solutions.

MINIMUM QUALIFICATIONS

An intermediate level of knowledge of UNIX (as defined in SAGE booklet).

Practical experience in computer security in a heterogeneous wide-area network.

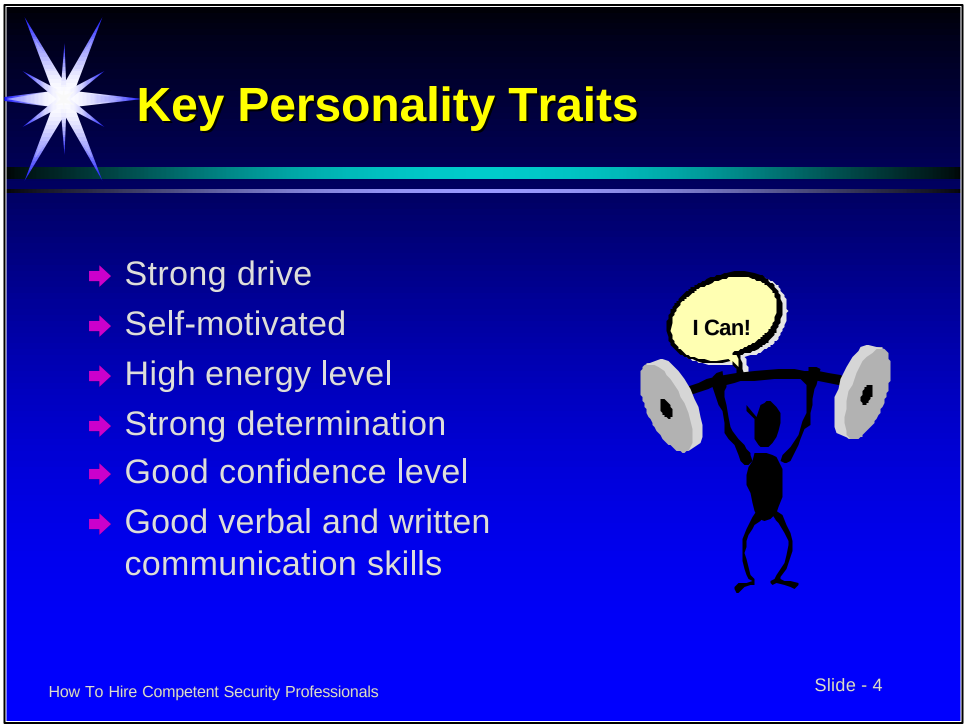
Familiarity with common break-in mechanisms and vulnerabilities of UNIX systems and be experienced in the application of procedures for resolving and mitigating network security threats.

Knowledge and experience of TCP/IP networks, Understanding of the OSI seven layer model.

An intermediate level of knowledge of C and shell programming languages, with a good understanding of Makefiles.

Good interpersonal skills enabling interaction with a diverse customer base and the ability to manage priorities with assigned responsibilities.

A BS/BA in Computer Science or associated degree and three to five years experience in a heterogeneous UNIX support environment.



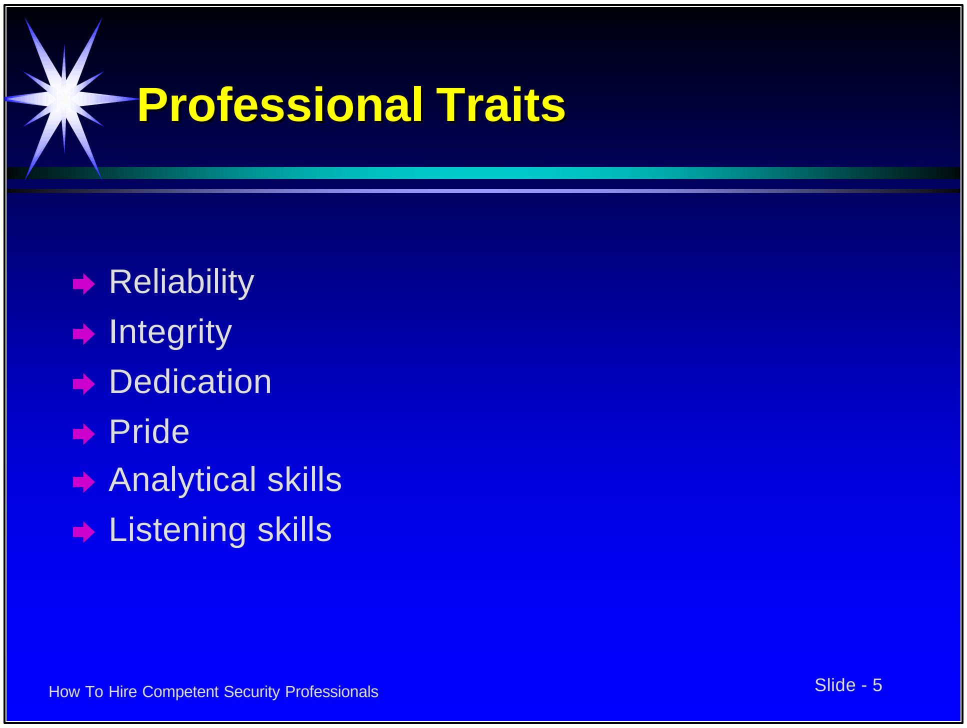
Key Personality Traits

- Strong drive
- Self-motivated
- High energy level
- Strong determination
- Good confidence level
- Good verbal and written communication skills

Notes:

People who have a lot of drive are strong self-starters and are usually motivated to get the work done on their own without a lot of prodding from management or other team members.

Good verbal and written communications skills are crucial in a support environment which requires a lot of interaction with the customers/users.



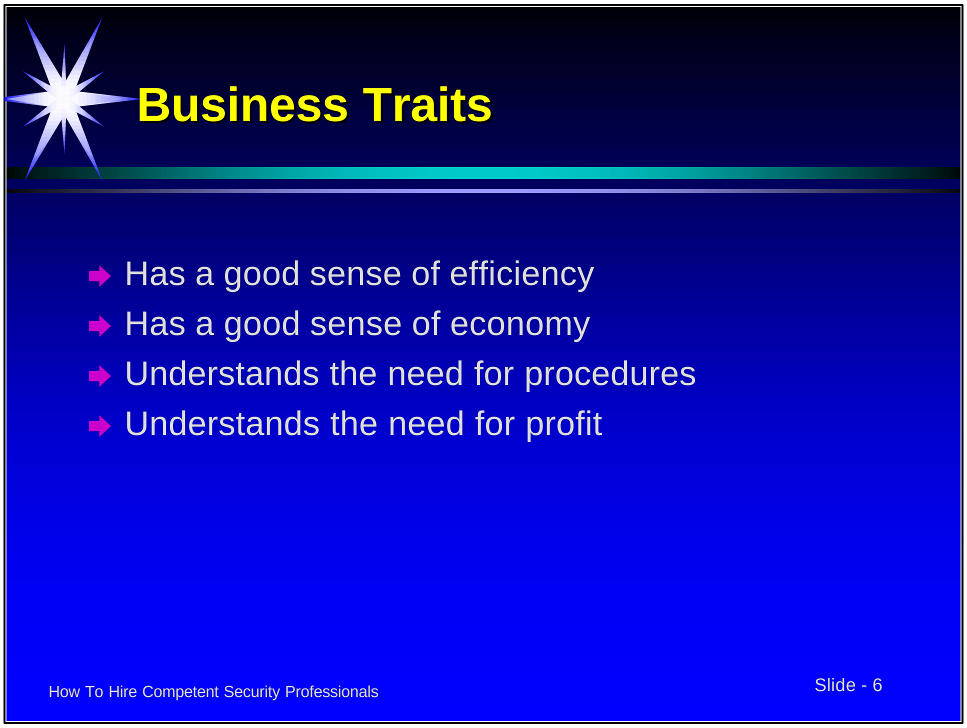
Professional Traits

- Reliability
- Integrity
- Dedication
- Pride
- Analytical skills
- Listening skills

Notes:

The profession traits will answer such questions as:

Will they get the job done?
Will they do the right thing?
Will they keep management informed when they should?
Will they answer pages at 3:00am?
Will they go above and beyond the call of duty to meet a tight deadline?
Do they care about the end result of their work?
Can they develop good solutions?
Will they listen other peoples views and concerns?



Business Traits

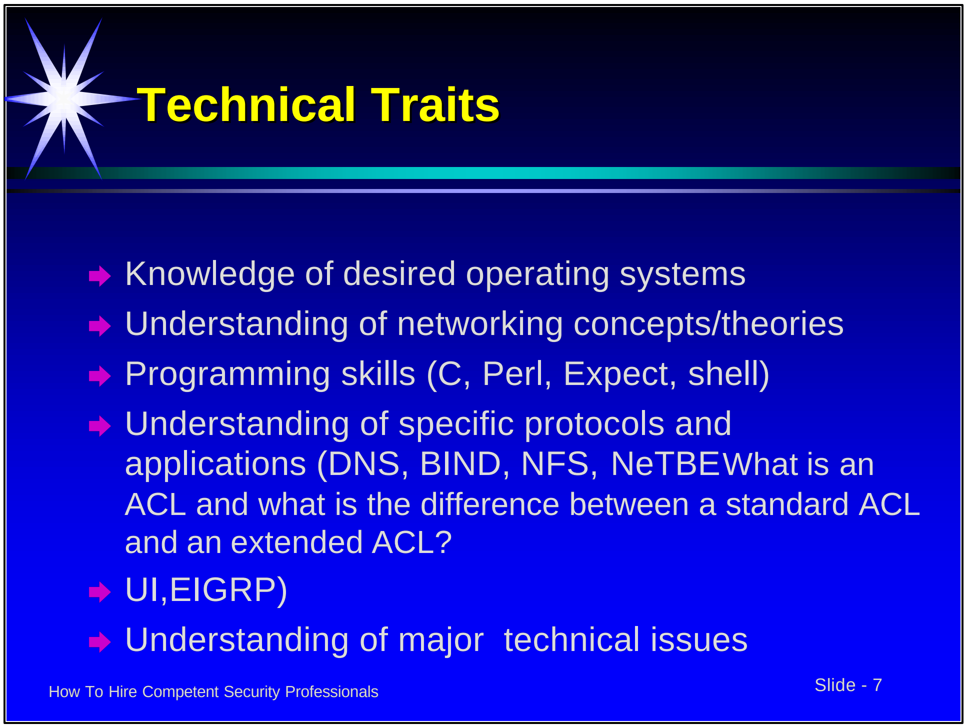
- Has a good sense of efficiency
- Has a good sense of economy
- Understands the need for procedures
- Understands the need for profit

Notes:

The business traits will answer such questions as:

Will they look for ways to improve processes and procedures to decrease waste of time and money?

Will they choose efficient solutions that scale over time versus an quick and easy solution?



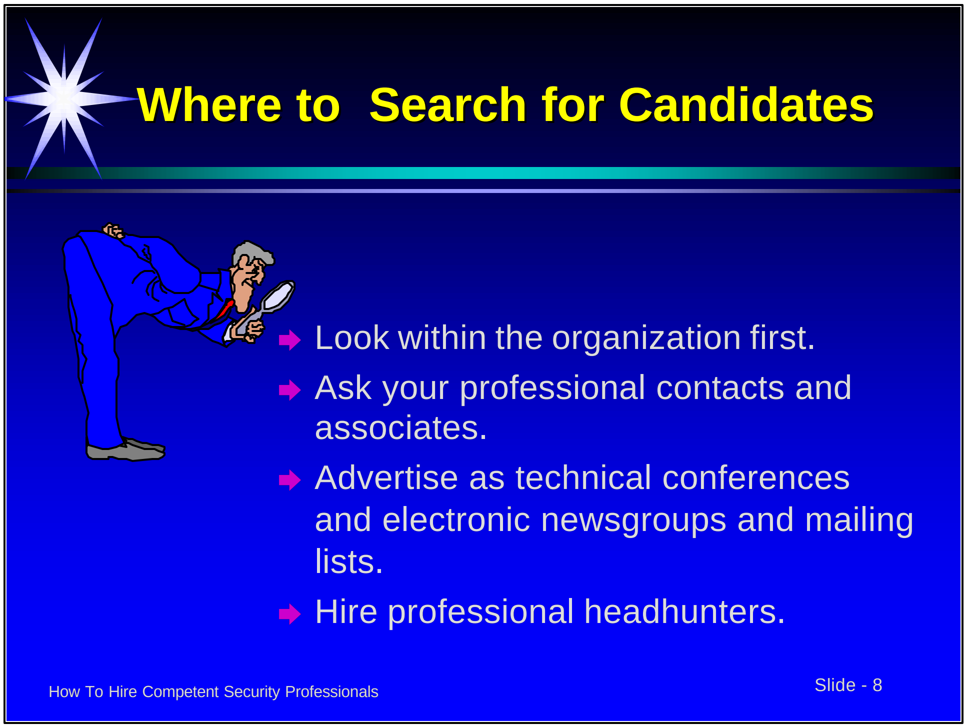
Technical Traits

- Knowledge of desired operating systems
- Understanding of networking concepts/theories
- Programming skills (C, Perl, Expect, shell)
- Understanding of specific protocols and applications (DNS, BIND, NFS, NeTBEWhat is an ACL and what is the difference between a standard ACL and an extended ACL?
- UI,EIGRP)
- Understanding of major technical issues

Notes:

The required technical traits will vary greatly from one job to the next. Security support encompasses an wide variety of tasks from low-level operational type tasks to consulting level tasks. Have the technical trait requirements match the position.

Try to separate out the “must-haves” versus “nice to have”.



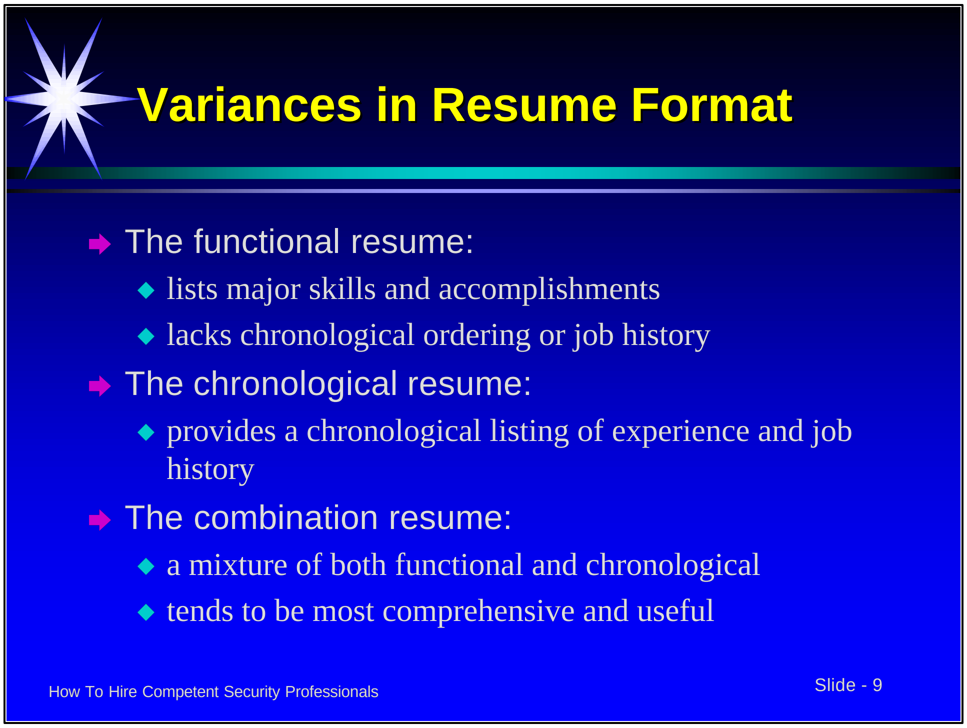
Where to Search for Candidates

- Look within the organization first.
- Ask your professional contacts and associates.
- Advertise as technical conferences and electronic newsgroups and mailing lists.
- Hire professional headhunters.

Notes:

It is best to look within the organization before looking elsewhere. Often companies will spend a lot of time and effort trying to find the right candidate, when all along they were in the office next door.

The number of available job positions far outweigh the number of available (and desirable) applicants. Some positions may bring in a few resumes, while others will bring in dozens.



Variances in Resume Format

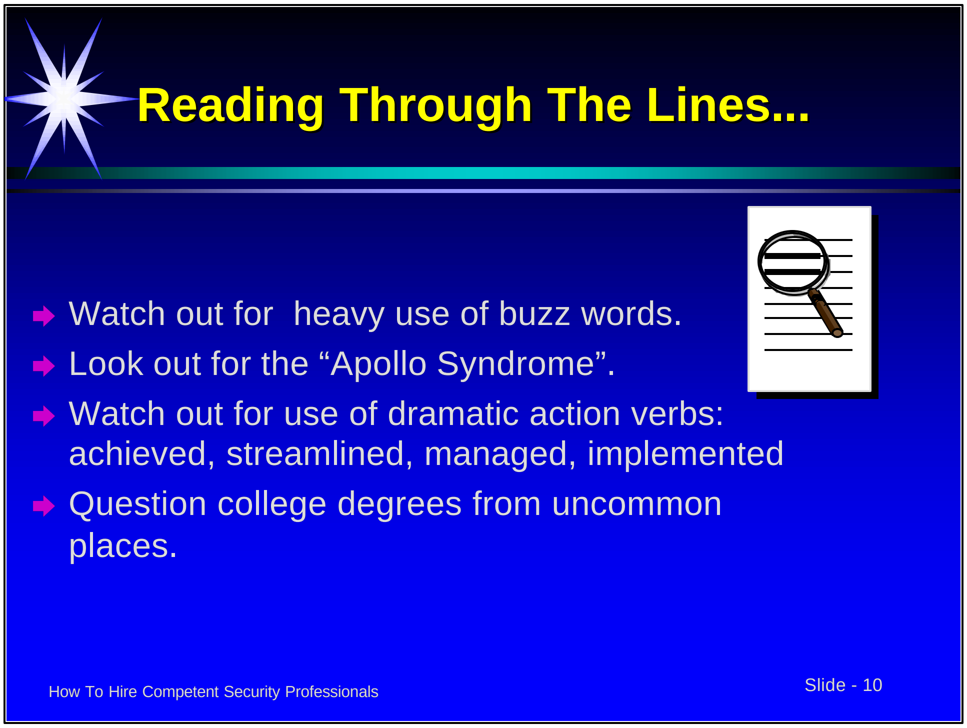
- The functional resume:
  - lists major skills and accomplishments
  - lacks chronological ordering or job history
- The chronological resume:
  - provides a chronological listing of experience and job history
- The combination resume:
  - a mixture of both functional and chronological
  - tends to be most comprehensive and useful

Notes:

The chronological resume is the most common. It provides a nice overview of job history and skills.

The functional resume is often used by senior professionals to keep their resumes to a manageable length. The format is also used by people who wish to hide gaps in their employment history or skills.

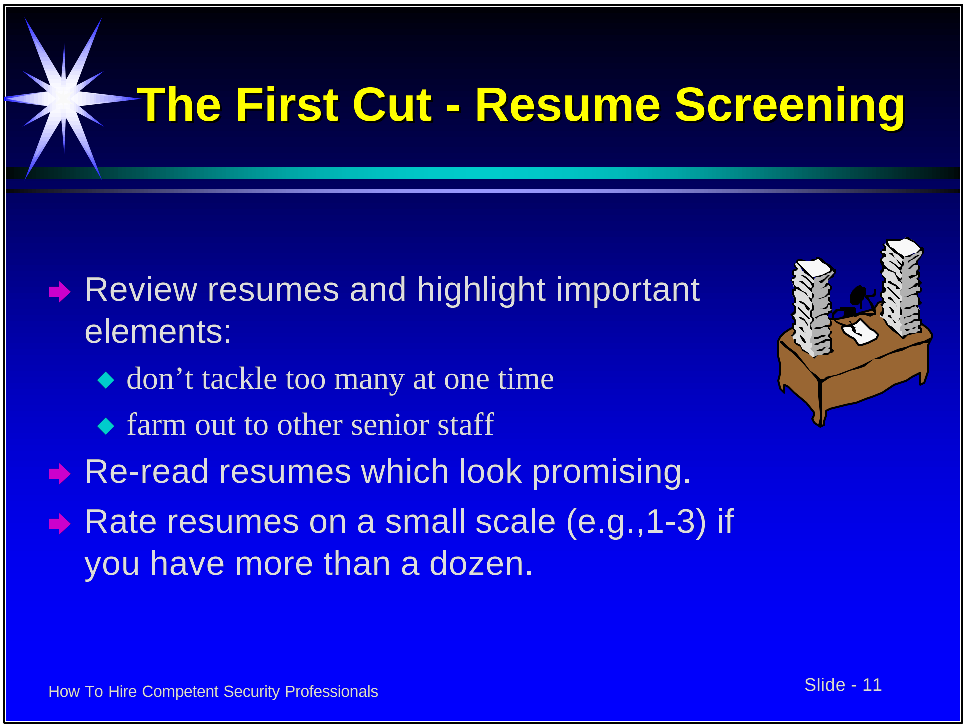
The combination resume combines the best elements of both.



Reading Through The Lines...

- Watch out for heavy use of buzz words.
- Look out for the “Apollo Syndrome”.
- Watch out for use of dramatic action verbs: achieved, streamlined, managed, implemented
- Question college degrees from uncommon places.

Notes:

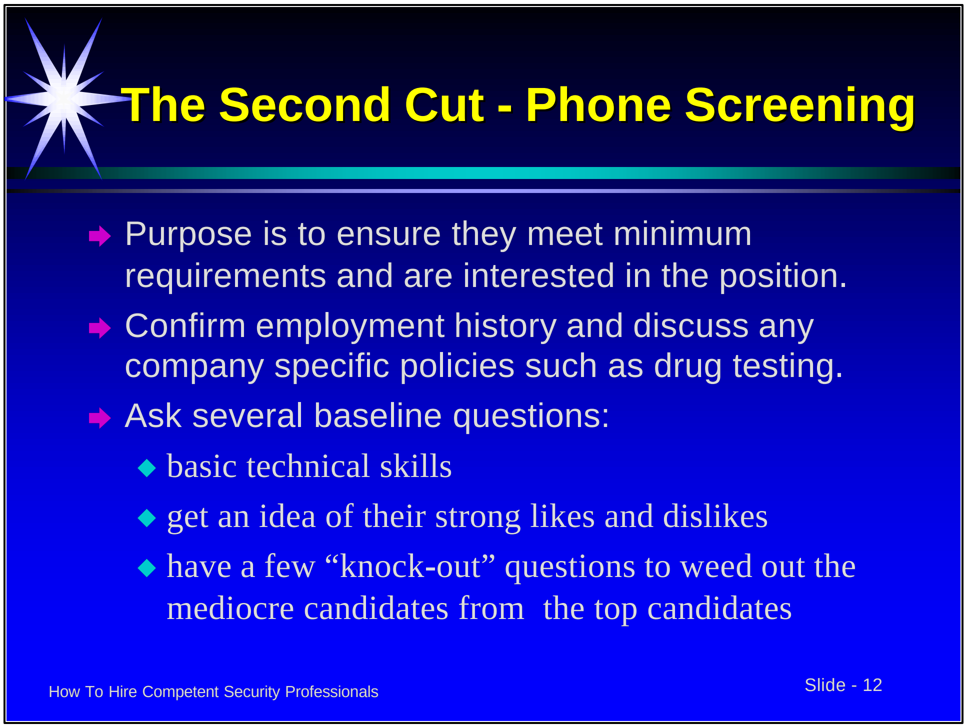


The First Cut - Resume Screening

- Review resumes and highlight important elements:
  - don’t tackle too many at one time
  - farm out to other senior staff
- Re-read resumes which look promising.
- Rate resumes on a small scale (e.g.,1-3) if you have more than a dozen.

Notes:

Many of the large companies and organizations use computerized resume scanning for the first round which can greatly reduce the number of resumes that actually get passed on to you.



The Second Cut - Phone Screening

- Purpose is to ensure they meet minimum requirements and are interested in the position.
- Confirm employment history and discuss any company specific policies such as drug testing.
- Ask several baseline questions:
  - basic technical skills
  - get an idea of their strong likes and dislikes
  - have a few “knock-out” questions to weed out the mediocre candidates from the top candidates

Notes:

Example Phone Screen Questions:

How many years of UNIX (or Win/NT) experience do you have?

How would you rate your UNIX (or Win/NT) skills on a level of 1 to 10?

Are you familiar with C, Perl or Bourne shell programming?

When was the last time you wrote a complex program from scratch?

What UNIX platforms to you have experience with? Was this at the user level or support level?

What versions of NT do you have experience with?

Can you describe to me what inetd is?

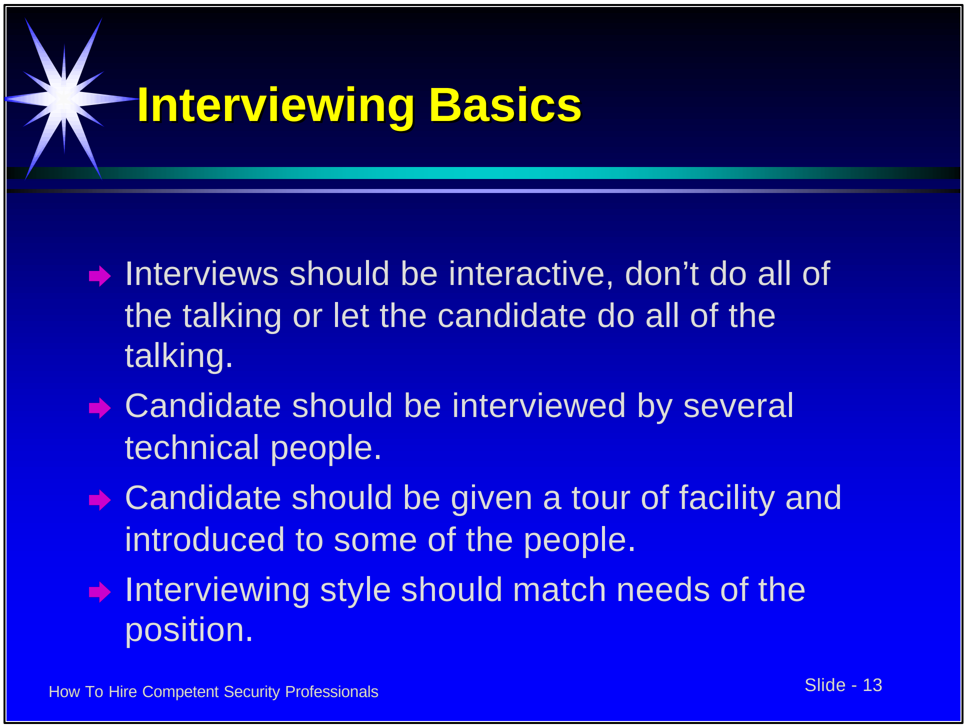
What is NetBEUI?

Can you tell me what system facility is use to log system messages?

What is your educational background?

Why are you interested in this position?

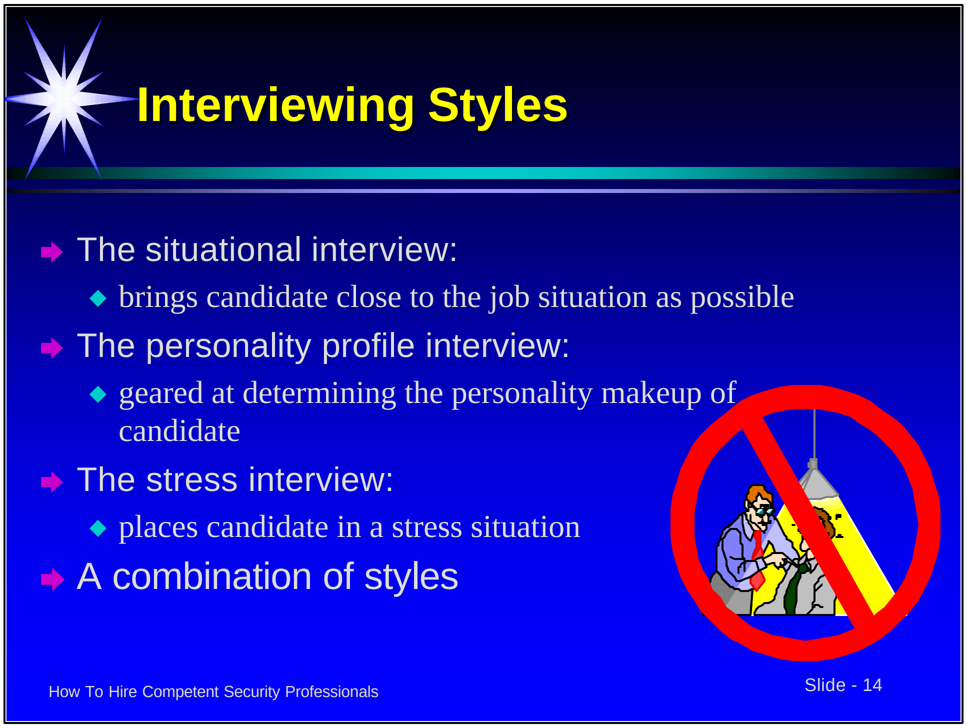
What was the most challenging project you worked on in the last year?



Interviewing Basics

- Interviews should be interactive, don't do all of the talking or let the candidate do all of the talking.
- Candidate should be interviewed by several technical people.
- Candidate should be given a tour of facility and introduced to some of the people.
- Interviewing style should match needs of the position.

Notes:



Interviewing Styles

- The situational interview:
  - brings candidate close to the job situation as possible
- The personality profile interview:
  - geared at determining the personality makeup of candidate
- The stress interview:
  - places candidate in a stress situation
- A combination of styles

Notes:

Remember, the interview is not an interrogation!

A combination of interviewing styles works best for a technical support position.

Situational interviews are excellent for positions which incur a lot of pressure or interaction with other people/groups/systems.

Some questions to ask in a personality profile interview:

How important was communication and interaction with others on the job?

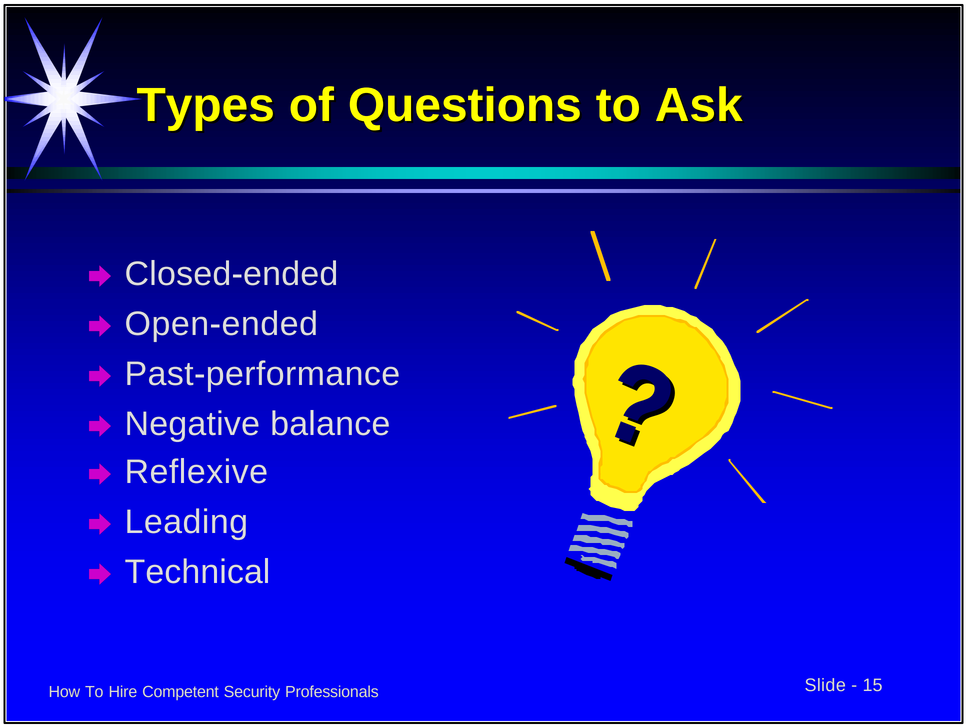
Do you enjoy working with other people with similar interests a you?

Do you enjoy working in a team atmosphere or would you consider yourself to be more of a loaner?

In the past, when you had difficulty dealing with a coworker, how did you resolve the situation?

How would you rank yourself among your current peers?

When beginning to work with new people on a task



Types of Questions to Ask

- Closed-ended
- Open-ended
- Past-performance
- Negative balance
- Reflexive
- Leading
- Technical

Notes:

Closed-ended questions are the most common, but not the best type.

Open-ended questions give the candidate an opportunity to expand on their answers.

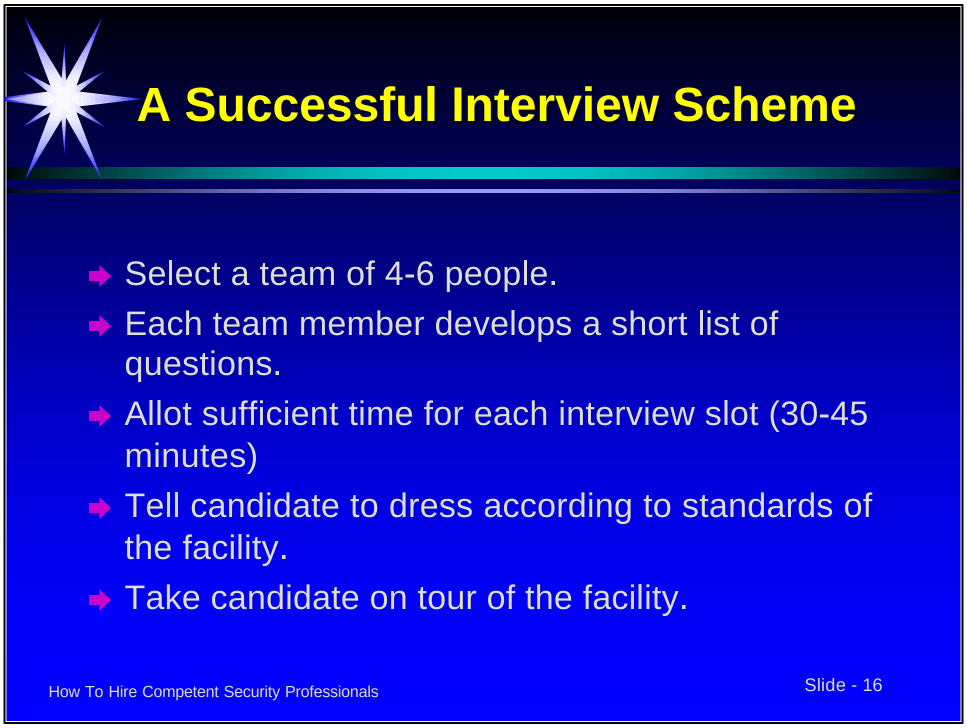
Past-performance questions require the candidate to focus on specific accomplishments and skills.

Negative balance questions help a candidate balance good skills and experience with less desirable traits or accomplishments.

Reflexive questions help the interviewer maintain control over the conversation and can act as topic closures.

Leading questions attempt to lead the candidate to a specific answer.

Technical questions test their true technical skills and understanding.



A Successful Interview Scheme

- Select a team of 4-6 people.
- Each team member develops a short list of questions.
- Allot sufficient time for each interview slot (30-45 minutes)
- Tell candidate to dress according to standards of the facility.
- Take candidate on tour of the facility.

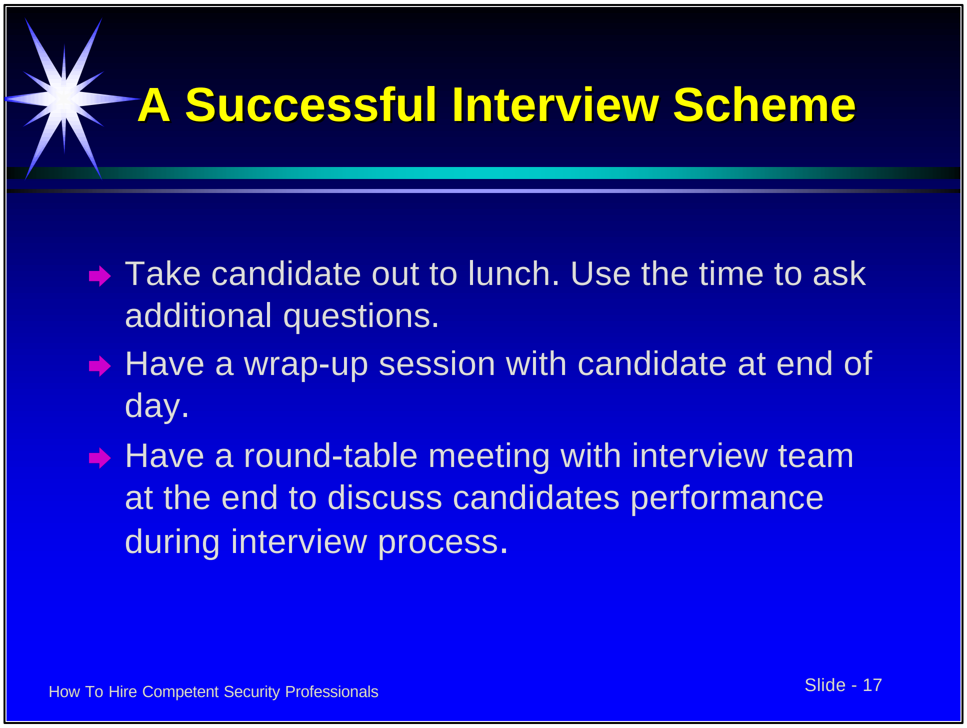
Notes:

Start interview process around 9:00am and finish around 3:00pm.

Members of the interview team should focus on difference areas such as programming, networking topics, general UNIX questions, etc.

The same set of questions should be used for each candidate interviewing for the same position.

If you have two or more junior people on your team, have them do a group interview.



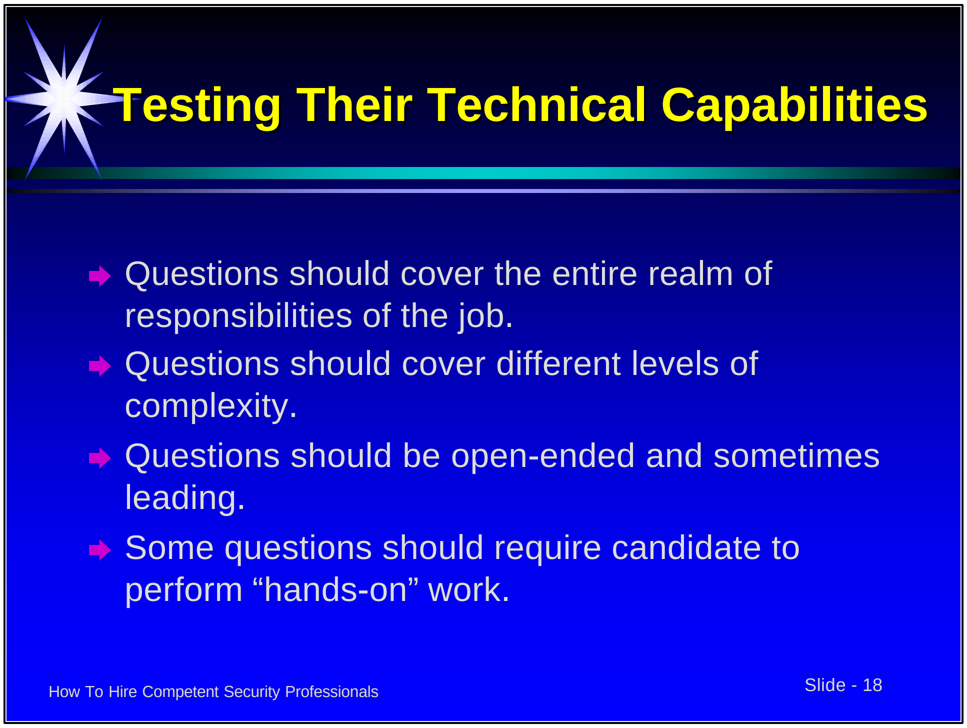
A Successful Interview Scheme

- Take candidate out to lunch. Use the time to ask additional questions.
- Have a wrap-up session with candidate at end of day.
- Have a round-table meeting with interview team at the end to discuss candidates performance during interview process.

Notes:

Use the wrap-up session to provide candidate an opportunity to ask any final questions. Ask candidate their interest level now that interview process has been completed.

Have the interview team fill out the candidate evaluation form, if required at your company/organization.



Testing Their Technical Capabilities

- Questions should cover the entire realm of responsibilities of the job.
- Questions should cover different levels of complexity.
- Questions should be open-ended and sometimes leading.
- Some questions should require candidate to perform “hands-on” work.

Notes:

Some technical questions used in our scheme:

How could you print out the first and third fields of the /etc/passwd file in a nice format?

What system call does the shell use to run a program?

What system utility is used to log system messages? How does this utility know what to log and where to log it?

What is an RFC? Where do you get one?

Write a shell for-loop which takes input from a text file containing a list of file names, and then performs an operation on those files?

What is the purpose of the inetd program? What are some of the other programs/daemons associated with inetd?

What are the main difference between a network based-auditing tool and a host-based auditing tool?

What type of attack program is land.c?

What is an ACL and what is the difference between a standard ACL and an extended ACL? Where do you apply an ACL?

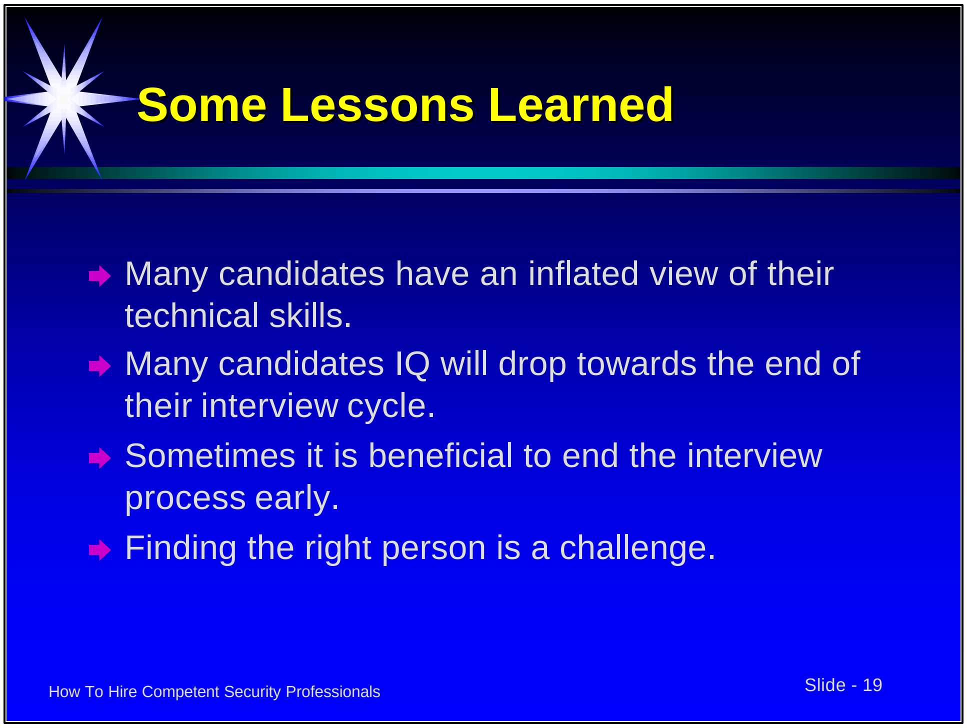
What did the program called Malissa do?

What typically runs on ports 53 and 80?

What are some major differences between TACACS+ and RADIUS?

What are some common uses for SSL based applications?

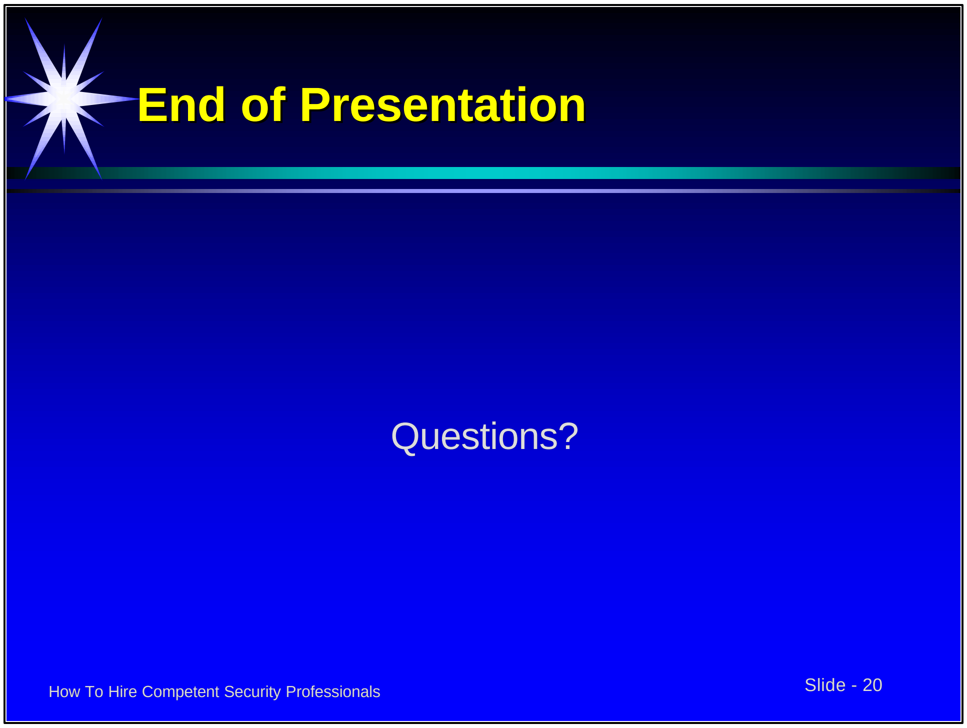
What does Net BUI mean and why would you want to use it?



Some Lessons Learned

- Many candidates have an inflated view of their technical skills.
- Many candidates IQ will drop towards the end of their interview cycle.
- Sometimes it is beneficial to end the interview process early.
- Finding the right person is a challenge.

Notes:



End of Presentation

Questions?

Notes: